



MOTOROLA
intelligence everywhere™

Booklet 3-6 of Volume 3

**ASTRO® 25 Digital Trunking Solutions
System Release 6.1**

Managing Network Transport Equipment



**68P81003Y54-O
November 2002**

Computer Software Copyrights

The Motorola products described in this document include a copyrighted Motorola computer program. Laws in the United States and other countries, as well as International Treaties, preserve for Motorola the exclusive rights for Motorola's copyrighted computer programs, including the exclusive right to copy, reproduce, distribute, or otherwise transfer said computer program(s). Accordingly, the copyrighted Motorola computer programs contained in this document may not be copied, decompiled, reverse engineered, or reproduced in any manner and on or within any media without the express written permission of Motorola. Furthermore, the purchase of Motorola products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents, or patent applications of Motorola, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Document Copyrights

© Motorola, Inc. All rights reserved.

No duplication or distribution of this document or any portion thereof shall take place without the express written permission of Motorola. No part of this document may be reproduced, distributed, or transmitted in any form or by any means, electronic or mechanical, for any purpose without the express written permission of Motorola.

To order additional copies of this document contact your Motorola sales representative.

Disclaimer

The information in this document is carefully examined, and is believed to be entirely reliable. However, no responsibility is assumed for inaccuracies. Furthermore, Motorola reserves the right to make changes to any products herein to improve readability, function, or design. Motorola does not assume any liability arising out of the applications or use of any product or circuit described herein; neither does it cover any license under its patent rights nor the rights of others.

Trademark Information

The following are registered trademarks of Motorola, Inc.: ASTRO, ASTRO-TAC, EMBASSY, FLASHport, FULLVISION, INTELLIREPEATER, MAXTRAC, Motorola, the Motorola logo, MSF 5000, PSC 9600, QUANTAR, QUANTRO, SECURENET, SMARTNET, SMARTZONE, SPECTRA, and STARTSITE.

The following are Motorola trademarks: CENTRACOM Series, CENTRACOM Gold Series, CENTRACOM Series II, CENTRACOM Series II Plus, Cisco, CoveragePLUS, DIGITAC, DVP, Max-Fax, MDC-600, Micor, MOSCAD, MSF 10000, MTS 2000, Private Conversation, SABER, SMARTNET II, SmartWorks, and Wireless Network Gateway.

HP, HP-UX, and Hewlett Packard are registered trademarks of Hewlett-Packard Corporation.

UNIX is a registered trademark of The Open Group in the United States and other countries.

PICMG, CompactPCI, and the PICMG and CompactPCI logos are registered trademarks of the PCI Industrial Computers Manufacturers Group.

PowerPC is a registered trademark of IBM in the United States.

Any other brand or product names are trademarks or registered trademarks of their respective holders.

WARRANTY

Limited Software Warranty

For the first ninety (90) days following its initial shipment, Motorola warrants that when properly used, its software will be free from reproducible defects that cause a material variance from its published specification. However, Motorola does not warrant that program operation will be uninterrupted or error-free, that each defect will be corrected, or that any program will meet Licensee's particular requirements.

This warranty does not cover an item of Software (i) used in other than its normal and customary manner; (ii) subjected to misuse; or (iii) subjected to modifications by Licensee or by any party other than Motorola without the prior written consent of Motorola.

Limited Media Warranty

For the first ninety (90) days following its initial shipment, Motorola warrants that the media carrying the software will be free from defects that damage the performance of the software. Motorola will replace any damaged media free of charge during the warranty period. Warranted media is limited to that which is used to transport the software (such as floppy disks and authorization key). PROMs that may store the software in equipment are not covered under this warranty.

Limitation of Liability

Motorola's total liability and Licensee's sole remedy for any warranted software shall be limited to, at Motorola's option, software replacement or the payment of Licensee's actual damages, not to exceed the total licensed charge paid by Licensee to Motorola for the item of software that caused the damage.

The warranties set forth above extend only to the first licensee. Subsequent transferees accept these programs "as is" and without warranties of any kind. **This warranty is given in lieu of all other warranties, express or implied, including, without limitation, the warranties of merchantability and fitness for a particular purpose.**

In no event shall Motorola be liable for special, incidental, or consequential damages (including, without limitation, loss of use, time or data, inconvenience, commercial loss, and lost profits or savings) to the full extent that such may be disclaimed by law even if Motorola has been advised of the possibility of such damage against licensee by any other party.

Repair of Defects

The classification of defects in Motorola-supplied software shall be the responsibility of Motorola. Remedy of defects is at the sole discretion of Motorola. If Motorola agrees to remedy a software defect, the new software will be warranted until the end of the original limited warranty period. Replacement of any software defect shall constitute Motorola supplying the Licensee with the appropriate software media and authorization key. Field installation and configuration are not included. Field software updates/upgrades and new enhancement option software will be warranted for ninety (90) days from the date of initial shipment.

All warranty service will be performed at service locations designated by Motorola. Travel and associated expenses of the Licensee or such expenses incurred by Motorola for visits to Licensee's location by Motorola personnel are not covered by this warranty.

Contents

Managing Network Transport Equipment

Chapter 1: Managing the LAN Switch

Managing Security Access	1-2
Viewing Account Permissions	1-3
Master Site System Diagram	1-4
Accessing CiscoWorks2000	1-5
Access Points for CiscoWorks2000	1-5
Launching CiscoWorks2000	1-6
Exiting CiscoWorks2000	1-9
Using CiscoView	1-9
CiscoView Features	1-9
Embedded CiscoView	1-10
Accessing CiscoView and CiscoView Commands	1-11
Viewing System Information	1-14
Viewing the System Time	1-15
Displaying VLAN Members	1-17
Monitoring the Performance of Ethernet Ports	1-19
Creating and Monitoring System Logs	1-22
Creating System Logs	1-23
Monitoring a System Log	1-26
Disabling the System Log	1-26
Monitoring the Performance of a LAN Switch	1-27
Monitoring the Performance of MSFC Routers	1-31
Using CiscoView for Fault Management	1-33
Using Resource Manager Essentials	1-35
RME Features	1-35
Overview of Procedures	1-35
Accessing Resource Manager Essentials	1-36
Resource Manager Essentials Applications	1-37
Viewing the LAN Switch Configuration	1-39
Backup and Restore Guidelines	1-41
Backing Up the LAN Switch Software and Configuration	1-42
Restoring the LAN Switch Software and Configuration	1-42
Transferring New Software to the LAN Switch	1-49
Copying the Catalyst Image Files to the TNM Client and the Server	1-50
Adding New Images to the Library	1-52
Distributing Software Images to the LAN Switch or MSFC Routers	1-54
Verifying the Software Image Distribution	1-58
Checking Device Configuration Changes and CiscoWorks2000 Users Who Made Changes	1-58

Checking Device Configuration Changes (Example 1)	1-59
Checking Device Configuration Changes (Example 2)	1-63
Verifying CiscoWorks2000 Users Who Made Configuration Changes	1-65
Displaying LAN Switch Alarms in HP OpenView	1-66

Chapter 2: Managing the WAN Switch

Managing Security Access	2-2
System Diagram.	2-4
Accessing Preside MDM.	2-4
Access Points for Preside MDM	2-5
Launching Preside MDM - Client Workstation	2-6
Menu Options	2-7
Relaunching Preside MDM - Client Workstation	2-8
Exiting Preside MDM	2-8
Obtaining the WAN Switch Name	2-8
Performing Inventory on the WAN Switch	2-9
Backing Up and Restoring the WAN Switch.	2-11
Obtaining the Provisioning Mode	2-13
Manually Backing Up the WAN Switch.	2-14
Restoring the WAN Switch	2-16
Downloading Software to the WAN Switch	2-18
Obtaining the New Software	2-19
Downloading the Software.	2-20
Adding a WAN Switch.	2-23
Logging On as Administrator	2-24
Selecting the Network Type	2-24
Adding a WAN Switch for Preside MDM to Manage	2-25
Adding WAN Switches to the Configuration Files	2-27
Verifying the WAN Switch Addition	2-28
Connecting to the WAN Switch by Command Line	2-29
Connecting to the WAN Switch Using Command Line Via Client Workstation.	2-30
Adding Prefixes.	2-33
Collecting and Displaying Performance Information	2-34
Useful Commands for Performance Viewer	2-37
Viewing the Status of WAN Switch Components	2-38
Accessing Component Information Viewer	2-41
Displaying WAN Switch Alarms	2-42
Displaying Alarms Using HP OpenView	2-43
Displaying Alarms using Preside	2-43
Using Preside MDM for Fault Management	2-44
Resetting a Card on the WAN Switch.	2-45
Using the MDMWeb	2-47
Overview of MDMWeb	2-47
Menu Options.	2-48
Access Points for MDMWeb.	2-49
Accessing MDMWeb	2-50
Navigating in MDMWeb	2-52
How to Correct Access Problems (Example Procedure)	2-53
Connecting to the WAN Switch Using Command Line Via MDMWeb	2-53
Displaying a Component List for the WAN Switch (Example Procedure)	2-55
Displaying Alarms Using MDMWeb	2-55
Displaying Alarms Using MDMWeb (View all Active Alarms).	2-55
Displaying Alarms Using MDMWeb (View Alarms by Severity)	2-56

Chapter 3: Managing the Routers

Overview of Tasks	3-1
Applicable Management Tasks for Selected Routers or Groups	3-2
Related Information in this Document Set	3-2
System Diagram	3-3
Accessing the Router Manager UI	3-5
Logging Out of Router Manager	3-7
Managing Groups	3-7
Building Default Groups	3-7
Adding and Deleting Routers	3-9
Preparing the Routers for Management	3-9
Adding Routers	3-10
Deleting Routers	3-12
Performing Router Management Functions	3-13
Downloading Files to Routers	3-14
Capturing (Uploading) Files From Routers	3-16
Viewing Runtime Logs	3-18
Viewing the Session Log	3-19
Viewing the Full Log	3-19
Viewing Daily Server Log Files	3-19
Backing Up Router Manager Data Files on the FullVision INM Server	3-21
Restoring Router Manager Data Files to the FullVision INM Server	3-23
Rebooting Routers	3-25
Performing Immediate Reboots	3-25
Performing Scheduled Reboots	3-27
Canceling Scheduled Reboots	3-32
Setting the Boot Block (Reboot Directory)	3-32
Viewing Router Information and Launching Configuration Applications	3-33
Performing Checksums	3-37
Canceling Router Manager Operations	3-39
Upgrading EOS Software on Routers in the Field	3-40
Downloading the New EOS Software to the Primary Directory	3-41
Rebooting the Routers and Verifying the Software Upgrade	3-43
Downloading the EOS Software to the Secondary Directory	3-44
Using the Portal to Upgrade EOS Firmware with Router Manager	3-45
General Procedure for Upgrading Router Firmware Using the Portal with Router Manager	3-46
Firmware Upgrade Issues	3-47
Portal Software Overview	3-48
Detailed Procedure for Upgrading Router Firmware Using the Portal with Router Manager	3-49
Verifying the Boot Source of the Router	3-50
Downloading the Portal Boot Image to the Secondary Boot Directory	3-51
Downloading the New Boot Image to the Primary Boot Directory	3-52
Rebooting the Routers with the Rebranded Boot Image	3-53
BCUB File Format	3-54
Using WEBLink	3-54
Key Differences Between WEBLink and Router Manager	3-55
Launching WEBLink	3-55
Viewing Performance Reports	3-58
Viewing Router Configuration	3-59

Chapter 4: Managing the Remote Terminal Server

Diagram of Typical Connections to the Remote Terminal Server	4-2
Reasons for Using the Remote Terminal Server	4-3
Process for Using the Remote Terminal Server	4-4

Remote Terminal Server Command Keys	4-5
Logging On to the Remote Terminal Server	4-6
Dialing In to the Terminal Server	4-7
Accessing the Terminal Server Through Telnet	4-8
Using the Remote Terminal Server to Access a Device	4-10
Opening Sessions with a Number of Devices	4-12
Opening a Telnet Session with a Host	4-13
Fixing Overlapping Lines in ProComm	4-13
Resuming a Session with a Device	4-14
Displaying All Remote Terminal Server Users	4-15
Accessing the Terminal Server Maintenance Environment	4-16
Disconnecting a Device Session	4-17
Logging Out of the Terminal Server	4-18
Viewing the Remote Terminal Server Configuration	4-19
Backing Up and Restoring the Remote Terminal Server	4-19
Backing Up the Terminal Server OS, Parameter File, and Menu File	4-20
Restoring the Terminal Server OS, Parameter File, and Menu File	4-24
Restoring Factory Defaults	4-24
Restoring the Parameter and Menu Files from Factory Defaults	4-26
Upgrading/Restoring the Load and Image Files	4-29

Chapter 5: Managing Other Transport Equipment

Managing Configuration Data	5-1
Backing Up Configuration Data	5-2
Three-Copy Backup Rule	5-2
Common Setup Procedures	5-3
Setting Up Microsoft HyperTerminal Software	5-3
Installing the 3Com TFTP Server Software	5-7
Setting Up TFTP	5-9
Managing the ARCA-DACS	5-10
Viewing the ARCA-DACS Configuration	5-10
Backing Up and Restoring the ARCA-DACS	5-13
ARCA-DACS Backup and Restore Requirements	5-13
Installing the Configuration Management Tool Software	5-14
Backing Up the ARCA-DACS	5-14
Restoring the ARCA-DACS	5-19
Managing the Channel Bank	5-25
Viewing the Channel Bank Configuration	5-26
Backing Up and Restoring the Channel Bank	5-26
Channel Bank Backup and Restore Requirements	5-26
Backing Up the Channel Bank	5-27
Restoring the Channel Bank	5-30
Managing the Digital Service Unit/Channel Service Unit	5-32
Viewing the Digital Service Unit/Channel Service Unit Configuration	5-32
Backing Up and Restoring the Digital Service Unit/Channel Service Unit	5-33
Backing Up the Digital Service Unit/Channel Service Unit	5-33
Restoring the Digital Service Unit/Channel Service Unit	5-33
Managing the HP Procurve Ethernet Switch	5-33
Viewing the Ethernet Switch Configuration	5-34
Backing Up and Restoring the Ethernet Switch	5-35
Ethernet Switch Backup and Restore Requirements	5-35
Backing Up the Ethernet Switch	5-35
Restoring the Ethernet Switch	5-37
Managing the Modem	5-38

Viewing the Modem Configuration	5-38
Backing Up and Restoring the Modem	5-39
Backing Up the Modem	5-40
Restoring the Modem	5-40
Managing the TRAK 9100	5-40
Viewing the TRAK 9100 Configuration.	5-41
Backing Up and Restoring the TRAK 9100	5-42

This page intentionally left blank.

List of Figures

Figure 1-1: Modify/Delete User Pane	1-3
Figure 1-2: Permissions Report Pane	1-4
Figure 1-3: System Diagram Example	1-5
Figure 1-4: Transport Network Management Applications Menu	1-5
Figure 1-5: Desktop Icon	1-6
Figure 1-6: CiscoWorks2000 Login Manager Pane	1-7
Figure 1-7: CiscoWorks2000 Main Window - Navigation Pane	1-8
Figure 1-8: CiscoView Main Window	1-11
Figure 1-9: Pop-Up Menu	1-12
Figure 1-10: System Information Dialog Box	1-14
Figure 1-11: Configure Device Dialog Box	1-15
Figure 1-12: Summer Time Dialog Box	1-16
Figure 1-13: Configure Device Dialog Box	1-17
Figure 1-14: VLAN & Bridge Category.	1-18
Figure 1-15: VLAN Ports	1-19
Figure 1-16: Ethernet Ports	1-20
Figure 1-17: Monitor Card Dialog Box	1-21
Figure 1-18: Monitor Card Dialog Box (showing example data)	1-22
Figure 1-19: Configure Device Dialog Box	1-23
Figure 1-20: System Log Dialog Box	1-24
Figure 1-21: Row Creation Dialog Box	1-24
Figure 1-22: System Log Dialog Box	1-25
Figure 1-23: Help Button	1-25
Figure 1-24: System Log Dialog Box - History	1-26
Figure 1-25: System Log Dialog Box	1-27
Figure 1-26: Monitor Device Dialog Box	1-28
Figure 1-27: CPU Utilization Dialog Box	1-29
Figure 1-28: CPU Utilization Dialog Box (showing example data)	1-30
Figure 1-29: MSFC Router Pop-up Menu	1-31
Figure 1-30: Monitor Card Dialog Box	1-32
Figure 1-31: Ethernet Module	1-34
Figure 1-32: Resource Manager Essentials Suite.	1-36
Figure 1-33: Search Archive by Device Dialog Box	1-39
Figure 1-34: Selected Devices List	1-40
Figure 1-35: Device Configuration Summary Report Dialog Box	1-40
Figure 1-36: Device Configuration Viewer Window	1-41
Figure 1-37: Backup and Restore LAN Switch Process Diagram	1-42
Figure 1-38: Search Archive by Device Dialog Box	1-43
Figure 1-39: Selected Devices List	1-44
Figure 1-40: Device Configuration Summary Report Dialog Box	1-44
Figure 1-41: Device Configuration Viewer Window	1-45
Figure 1-42: Config Editor Window	1-46

Figure 1-43: Config Editor Job Wizard	1-47
Figure 1-44: Job Properties Dialog Box	1-48
Figure 1-45: Browse Job Dialog Box	1-49
Figure 1-46: LAN Switch Software Management Process Diagram	1-50
Figure 1-47: Select Image Source Dialog Box	1-52
Figure 1-48: Select Image Type Dialog Box	1-52
Figure 1-49: Select Device Type Dialog Box	1-54
Figure 1-50: Select Catalyst Devices Dialog Box (Example)	1-54
Figure 1-51: Recommended Image Upgrade Dialog Box	1-55
Figure 1-52: Verify Image Upgrade Dialog Box	1-56
Figure 1-53: Job Control Information Dialog Box	1-57
Figure 1-54: Compare Configurations Dialog Box	1-59
Figure 1-55: Compare Configurations Dialog Box	1-60
Figure 1-56: Configuration Version Compare Report	1-61
Figure 1-57: Configuration Compare Report Dialog Box	1-62
Figure 1-58: Compare Configurations Dialog Box	1-63
Figure 1-59: Compare Configurations Dialog Box	1-64
Figure 1-60: Configuration Version Compare Report	1-64
Figure 1-61: Change Audit 24-Hour Report	1-65
Figure 2-1: System Diagram Example	2-4
Figure 2-2: Transport Network Management Applications Menu	2-5
Figure 2-3: Preside Client Access Desktop Icon	2-5
Figure 2-4: Preside MDM Main Window	2-6
Figure 2-5: Passport Inventory Tool Window	2-9
Figure 2-6: Passport Authentication Dialog Box	2-10
Figure 2-7: Passport Inventory Tool Window	2-10
Figure 2-8: Card Inventory Report Window	2-11
Figure 2-9: Preside Backup and Restore Process	2-12
Figure 2-10: Command Console Connection Management Dialog Box	2-14
Figure 2-11: Passport Service Data Backup Window	2-15
Figure 2-12: Passport Service Data Restore Window	2-17
Figure 2-13: Selective Restore Dialog Box	2-18
Figure 2-14: Preside Software Management Process	2-19
Figure 2-15: Command Console Connection Management Dialog Box	2-21
Figure 2-16: Passport Software Distribution & Configuration Window	2-22
Figure 2-17: SDS Authentication Dialog Box	2-22
Figure 2-18: Command Console Window	2-30
Figure 2-19: Command Console Connection Management Dialog Box	2-31
Figure 2-20: Command Console Connection Management Dialog Box	2-32
Figure 2-21: Prefix Definition Dialog Box	2-33
Figure 2-22: Performance Viewer Window	2-35
Figure 2-23: Displayed CPU and Memory Performance for a Card	2-36
Figure 2-24: Traffic Report	2-37
Figure 2-25: Network Viewer Window	2-39
Figure 2-26: Switch Level View	2-40
Figure 2-27: Status Dialog Box	2-41
Figure 2-28: Component Information Viewer Window	2-42
Figure 2-29: Alarm Display Window	2-44
Figure 2-30: Command Console Window	2-46
Figure 2-31: Transport Network Management Applications Menu	2-49
Figure 2-32: Desktop Icon	2-50
Figure 2-33: MDMWeb Login Page	2-50
Figure 2-34: MDMWeb Main Page	2-51
Figure 2-35: View of Managed WAN Switches in MDMWeb	2-52
Figure 2-36: Pop-Up Menu Available from Navigation Pane	2-53

Figure 2-37: Connection Management Window	2-54
Figure 2-38: Component List for the WAN Switch.	2-55
Figure 2-39: Alarm Display Window (All Active Alarms)	2-56
Figure 2-40: Alarm Display Window (Filtered by Severity)	2-57
Figure 3-1: System Diagram Example	3-4
Figure 3-2: Router Manager Welcome Window	3-5
Figure 3-3: Router Manager Main Window Elements	3-6
Figure 3-4: Build Default Groups Display.	3-8
Figure 3-5: Default Groups in Group Browser.	3-8
Figure 3-6: Zone Groups with Parts of Hierarchy Expanded in Group Browser	3-9
Figure 3-7: Router Manager Add Router Display	3-11
Figure 3-8: Router Manager View Router Display	3-12
Figure 3-9: Router Manager Data Flow Between PC, FullVision INM Server, and Routers	3-14
Figure 3-10: Router Manager Download Display	3-15
Figure 3-11: Router Manager Capture Display	3-17
Figure 3-12: Router Manager Session Log	3-19
Figure 3-13: View Server Log Submenu	3-20
Figure 3-14: View File Dialog Box	3-20
Figure 3-15: Router Manager Backup Display.	3-22
Figure 3-16: Router Manager Restore Display.	3-24
Figure 3-17: Router Manager Reboot Display	3-25
Figure 3-18: Router Manager Reboot Now+ Option	3-29
Figure 3-19: Router Manager Reboot At Option	3-30
Figure 3-20: Choose Reboot Time Dialog Box in Router Manager Reboot Window	3-31
Figure 3-21: Router Manager Reboot Display	3-32
Figure 3-22: Router Manager Set Boot Block Display	3-33
Figure 3-23: Router Manager View Router Display	3-35
Figure 3-24: Router Manager Perform Checksum Display	3-38
Figure 3-25: Making Selections on the Router Manager Download Display	3-42
Figure 3-26: Making Selections on the Router Manager Reboot Display.	3-43
Figure 3-27: Router Manager View Router Display	3-50
Figure 3-28: Configuring the Portal Software Download	3-51
Figure 3-29: Configuring the New Boot Image Download	3-52
Figure 3-30: Router Manager Reboot Display	3-53
Figure 3-31: View Router Display	3-56
Figure 3-32: WEBLink Main Interface Window	3-57
Figure 3-33: Performance Report Graph	3-58
Figure 3-34: Router Configuration Parameters.	3-59
Figure 4-1: Remote Terminal Server Connections	4-3
Figure 4-2: Accessing a Device Through the Terminal Server	4-4
Figure 4-3: Disconnecting Devices and Logging Out of the Remote Terminal Server.	4-4
Figure 4-4: 3CServer Window	4-22
Figure 4-5: 3CServer Window	4-28
Figure 5-1: Connection Description Dialog Box	5-4
Figure 5-2: Connect To Dialog Box.	5-5
Figure 5-3: Port Settings Tab.	5-6
Figure 5-4: Settings Tab	5-7
Figure 5-5: 3CServer Window	5-8
Figure 5-6: 3CServer Configuration	5-9
Figure 5-7: CMT Login Dialog Box	5-11
Figure 5-8: CMT Console Window	5-12
Figure 5-9: CMT Main Window (Shelf).	5-12
Figure 5-10: CMT Shortcut Icon	5-14
Figure 5-11: 3CServer Window	5-15
Figure 5-12: CMT Login Dialog Box	5-15

Figure 5-13: CMT Console Window	5-17
Figure 5-14: CMT Main Window (Shelf)	5-17
Figure 5-15: NVRAM Tab	5-18
Figure 5-16: Backup Progress	5-19
Figure 5-17: CMT Message Dialog Box	5-19
Figure 5-18: 3CServer Window	5-20
Figure 5-19: CMT Login Dialog Box	5-20
Figure 5-20: CMT Console Window	5-22
Figure 5-21: Shelf Window	5-22
Figure 5-22: NVRAM Tab	5-23
Figure 5-23: Warning Dialog Box	5-24
Figure 5-24: Restore Progress	5-25
Figure 5-25: CMT Message Dialog Box	5-25
Figure 5-26: Channel Bank Main Screen	5-26
Figure 5-27: Channel Bank Main Screen	5-27
Figure 5-28: Test and Debug Screen	5-28
Figure 5-29: NVRAM Backup Screen	5-28
Figure 5-30: Capture Text Menu	5-29
Figure 5-31: Channel Bank Login Screen	5-30
Figure 5-32: Channel Bank Main Screen	5-31
Figure 5-33: Console Main Menu	5-34
Figure 5-34: 3CServer Window	5-36
Figure 5-35: Console Main Menu	5-36
Figure 5-36: Telnet Screen	5-41
Figure 5-37: Setup Mode Screen	5-41

List of Tables

Table 1-1: Embedded CiscoView Features	1-10
Table 1-2: Overview of RME Procedures	1-35
Table 1-3: RME Applications	1-37
Table 1-4: Recommended Frequency of Backups and Restores	1-41
Table 2-1: Account Types for Client Access	2-2
Table 2-2: Account Types for Web Access	2-3
Table 2-3: Account Types for WAN Switch	2-3
Table 2-4: Menu Options for Preside MDM	2-7
Table 2-5: Recommended Frequency of Backup and Restores	2-11
Table 2-6: MDMWeb Menu Options	2-48
Table 3-1: Management Tasks	3-2
Table 3-2: View Router Display	3-34
Table 3-3: Comparison of PathBuilder, Portal, and Rebranded (ST) Firmware	3-48
Table 4-1: Remote Terminal Server Commands	4-5
Table 5-1: List of Backup Media Recommendations for Network Transport Devices	5-3

This page intentionally left blank.

List of Procedures

Procedure 1-1: How To View Account Permissions	1-3
Procedure 1-2: How to Launch CiscoWorks2000	1-7
Procedure 1-3: How to Exit CiscoWorks2000	1-9
Procedure 1-4: How to Access CiscoView and CiscoView Commands	1-11
Procedure 1-5: How to View the System Information	1-14
Procedure 1-6: How to View the System Time.	1-15
Procedure 1-7: How to Display VLAN Members	1-17
Procedure 1-8: How to Monitor the Performance of Ethernet Ports	1-20
Procedure 1-9: How to Create System Logs	1-23
Procedure 1-10: How to Monitor the System Log	1-26
Procedure 1-11: How to Disable the System Log	1-27
Procedure 1-12: How to Monitor the Performance of the LAN Switch	1-28
Procedure 1-13: How to Monitor the Performance of MSFC Routers	1-31
Procedure 1-14: How to Reset the Ethernet Module	1-34
Procedure 1-15: How to Access RME	1-36
Procedure 1-16: How to View the LAN Switch Configuration	1-39
Procedure 1-17: How to Restore an Old Configuration	1-43
Procedure 1-18: How to Copy the Catalyst Image Files to the TNM Client and the Server	1-51
Procedure 1-19: How to Add New Images to the Library.	1-52
Procedure 1-20: How to Distribute the Software Image to the LAN Switch or MSFC Routers.	1-54
Procedure 1-21: How to Verify the Software Image Distribution	1-58
Procedure 1-22: How to Check Device Configuration Changes (Example 1).	1-59
Procedure 1-23: How to Check Device Configuration Changes (Example 2).	1-63
Procedure 1-24: How to Verify the CiscoWorks2000 Users Who Made the Configuration Changes	1-65
Procedure 2-1: How to Launch Preside MDM	2-6
Procedure 2-2: How to Relaunch Preside MDM	2-8
Procedure 2-3: How to Exit Preside MDM	2-8
Procedure 2-4: How to Perform Inventory on the WAN Switch	2-9
Procedure 2-5: How to Obtain the Provisioning Mode	2-13
Procedure 2-6: How to Manually Back Up the WAN Switch	2-14
Procedure 2-7: How to Restore the WAN Switch	2-16
Procedure 2-8: How to Download Software to the WAN Switch	2-20
Procedure 2-9: How to Download Software	2-21
Procedure 2-10: How to Log On as Administrator	2-24
Procedure 2-11: How to Select the Network Type	2-25
Procedure 2-12: How to Add a WAN Switch for Preside MDM to Manage	2-25
Procedure 2-13: How to Add a WAN Switch to the Configuration File	2-27
Procedure 2-14: How to Verify the WAN Switch Addition	2-28
Procedure 2-15: How to Connect to the WAN Switch Using Command Line via Client Workstation.	2-30
Procedure 2-16: How to Add Prefixes	2-33
Procedure 2-17: How to Collect and Display Performance Information	2-35
Procedure 2-18: How to Check the Status of a WAN Switch Component	2-39

Procedure 2-19: How to Access the Component Information Viewer	2-42
Procedure 2-20: How to View Alarms on the WAN Switch	2-44
Procedure 2-21: How to Reset a Card on the WAN Switch	2-46
Procedure 2-22: How to Access the MDMWeb	2-50
Procedure 2-23: How to Navigate to Display the Managed Switches	2-52
Procedure 2-24: How to Correct Access Problems	2-53
Procedure 2-25: How to Connect to the WAN Switch Using Command Line Via MDMWeb	2-54
Procedure 2-26: How to Display a Component List for the WAN Switch	2-55
Procedure 2-27: How to Display Alarms Using MDMWeb (View all Active Alarms).	2-55
Procedure 2-28: How to Display Alarms Using MDMWeb (View Alarms by Severity).	2-56
Procedure 3-1: How to Access Router Manager	3-6
Procedure 3-2: How to Build Default Default Groups	3-8
Procedure 3-3: How to Add a Router	3-11
Procedure 3-4: How to Delete a Router	3-12
Procedure 3-5: How to Download Files from the FullVision INM Server to Routers	3-15
Procedure 3-6: How to Capture (Upload) Files from Routers to the FullVision INM Server	3-17
Procedure 3-7: How to View Daily Server Log Files	3-20
Procedure 3-8: How to Back Up Router Manager Data Files on the FullVision INM Server.	3-22
Procedure 3-9: How to Restore Router Manager Data Files to the FullVision INM Server	3-24
Procedure 3-10: How to Perform an Immediate Reboot	3-25
Procedure 3-11: How to Schedule a Router Reboot to Occur after a Specified Interval	3-28
Procedure 3-12: How to Schedule a Router Reboot to Occur at a Specified Time.	3-29
Procedure 3-13: How to Cancel a Scheduled Reboot.	3-32
Procedure 3-14: How to Set the Boot Block (Reboot Directory)	3-33
Procedure 3-15: How to View Router Information and Launch Configuration Applications	3-35
Procedure 3-16: How to Perform Checksum Calculations	3-38
Procedure 3-17: How to Cancel Router Manager Operations	3-40
Procedure 3-18: How to Download the New EOS Software to the Primary Directory.	3-41
Procedure 3-19: How to Reboot the Routers and Verify the Software Upgrade	3-43
Procedure 3-20: How to Download the EOS Software to the Secondary Directory	3-45
Procedure 3-21: How to Upgrade Router Firmware Using the Portal with Router Manager (General Procedure)	3-47
Procedure 3-22: How to Verify the Boot Source of the Router	3-50
Procedure 3-23: How to Download the Portal Boot Image to the Secondary Boot Directory.	3-51
Procedure 3-24: How to Download the New Boot Image to the Primary Boot Directory	3-52
Procedure 3-25: How to Reboot the Routers with the Rebranded Boot Image	3-53
Procedure 3-26: How to Launch WEblink	3-55
Procedure 3-27: How to View a Performance Report.	3-58
Procedure 3-28: How to View the Router Configuration	3-59
Procedure 4-1: How to Access the Terminal Server through Dial In	4-7
Procedure 4-2: How to Log On to the Remote Terminal Server	4-8
Procedure 4-3: How to Access a Device through the Remote Terminal Server	4-10
Procedure 4-4: How to Open Sessions with a Number of Devices.	4-12
Procedure 4-5: How to Open a Telnet Session with a User-Defined Host	4-13
Procedure 4-6: How to Fix Overlapping Lines in ProComm	4-13
Procedure 4-7: How to Resume an Opened Device Session.	4-14
Procedure 4-8: How to View All the Users Logged On to the Terminal Server	4-15
Procedure 4-9: How to Access the Terminal Server Maintenance Environment	4-16
Procedure 4-10: How to Disconnect a Session with a Device	4-17
Procedure 4-11: How to Log Out of the Terminal Server	4-18
Procedure 4-12: How to View the Remote Terminal Server Configuration.	4-19
Procedure 4-13: How to Back Up Terminal Server Files	4-21
Procedure 4-14: How to Restore Terminal Server to Factory Defaults	4-24
Procedure 4-15: How to Restore Files from Factory Defaults	4-27
Procedure 4-16: How to Upgrade/Restore Load and Image Files	4-30
Procedure 5-1: How to Set Up Microsoft HyperTerminal.	5-4

Procedure 5-2: How to Install 3Com TFTP Server	5-8
Procedure 5-3: How to Set Up TFTP	5-9
Procedure 5-4: How to View the ARCA-DACS Configuration	5-11
Procedure 5-5: How to Install the CMT Software	5-14
Procedure 5-6: How to Back Up the ARCA-DACS	5-15
Procedure 5-7: How to Restore the ARCA-DACS	5-20
Procedure 5-8: How to View the Channel Bank Configuration	5-26
Procedure 5-9: How to Back Up the Channel Bank	5-27
Procedure 5-10: How to Restore the Channel Bank	5-30
Procedure 5-11: How to View the Ethernet Switch Configuration	5-34
Procedure 5-12: How to Back Up the Ethernet Switch	5-35
Procedure 5-13: How to Restore the Ethernet Switch	5-37
Procedure 5-14: How to View the Modem Configuration.	5-39
Procedure 5-15: How to View the TRAK 9100 Configuration	5-41

This page intentionally left blank.

List of Processes

Process 1-1: Transferring New Software to the LAN Switch	1-50
Process 4-1: Restoring the Terminal Server OS, Parameter File, and Menu File	4-24

This page intentionally left blank.

Managing Network Transport Equipment

Network management software manages the components of a complex computer network in a radio system. These tools maximize available resources and minimize the system downtime and maintenance. This booklet discusses how to perform the tasks required to manage your network transport equipment using the following means:

- CiscoWorks2000 to manage the Cisco® Catalyst® 6509 Enterprise Ethernet Switch (LAN switch)
- Preside® MDM to manage the Nortel® Passport® 7480 WAN Switch (WAN switch)
- Router Manager to manage the Motorola® Network Router (MNR) S Series and ST5000 Series routers
- Remote terminal server to remotely access equipment
- Command line interfaces to manage LAN/WAN equipment

What is Covered In This Manual?

This booklet is organized as follows:

- Chapter 1, "Managing the LAN Switch." This chapter presents how to use CiscoWorks2000, including CiscoView and Resource Manager Essentials (RME), to manage the LAN switch.
- Chapter 2, "Managing the WAN Switch." This chapter presents how to use Preside MDM and MDMWeb to manage the WAN switch.
- Chapter 3, "Managing the Routers." This chapter describes how to use Router Manager and WEBLink to manage the MNR S series and ST5000 series routers.
- Chapter 4, "Managing the Remote Terminal Server." This chapter presents procedures to access, use, back up, and restore the remote terminal server.
- Chapter 5, "Managing Other Transport Equipment." This chapter presents procedures for backing up and restoring network transport devices other than the LAN switch, the WAN switch, or routers.

Helpful Background Information

You will find this booklet most helpful if you have already done the following:

- Read and understood Volume 1: *Understanding Your ASTRO 25 Trunking System*, for an overview about the system and the entire document set.
- Read and understood the CiscoWorks and Preside MDM user manuals and other documentation provided by the manufacturer.

- Read and understood the HP® OpenView® and Router Manager documentation provided by the manufacturer.

Related Information

Related Information	Purpose
Volume 1: <i>Understanding Your ASTRO 25 Trunking System</i>	An overview of the Network Transport applications: CiscoWorks2000, Preside MDM, InfoVista, and Router Manager.
Volume 2: <i>Fault Management</i>	Discusses how to use FullVision® Integrated Network Manager (INM). Includes the trap definitions for the LAN switch, WAN switch, and routers.
Volume 5,	Discusses the performance management aspects of the Network Transport Management applications, including how to view reports from InfoVista for the LAN switch, WAN switch, and routers.
Volume 9, <i>Master Site Hardware and Software Configuration</i>	Includes how to install and configure the routers and switches.
Volume 9, <i>Network Transport Applications Installation and Configuration</i>	Includes how to install and configure the Solaris® OS and the software for CiscoWorks2000 and Preside MDM. How to install and configure Windows® 2000 Server OS and InfoVista.
Volume 9, <i>Master Site Software Installation</i>	Includes how to install and configure Router Manager on the FullVision INM server.
FullVision INM Online help	Includes reference information for FullVision INM and Router Manager.

Component	Documentation
CiscoWorks2000	<ul style="list-style-type: none"> Reference documentation CD — includes all documentation in pdf format in the /doc folder. <i>CiscoWorks2000 User Manual</i> (HTML) — available online from the CiscoWorks2000 Help button. <i>CiscoWorks2000 Product Tutorial CD</i> — includes CD-One CiscoView and Resource Manager Essential. CiscoWorks Release Notes (HTML) — available online at www.cisco.com.
Preside MDM	<ul style="list-style-type: none"> Preside MDM 13.3 CD — includes all documentation in pdf format. Preside Online Help — available from the Help menu on the Preside MDM window or from MDMWeb: http://10.0.0.16:8080/WebNMS/WebNMS.html
Router Manager	Router Manager online help — available from the Help menu of the Router Manager UI.
WEBLink	Online help — available from the Help icon in the WEBLink navigation pane.
Routers	<p>Related DocumentationEOS Documents — available from the Help menu of the Router Manager UI, from the EOS Release CD, or from the WEBLink Documentation link. Includes the following:</p> <ul style="list-style-type: none"> <i>S Series S4000 Hardware User Guide</i> — provides instructions for installing a Motorola S Series S4000 router and performing basic device configuration. <i>ST5000 Series Hardware User Guide</i> — provides instructions for installing a Motorola ST5000 Series router and performing basic device configuration. <i>Enterprise OS Software User Guide</i> — provides information about how to use Enterprise OS (EOS) software to operate and configure your router. <i>Enterprise OS Software Reference Guide</i> — provides detailed information about commands and syntax for all EOS service parameters.
Remote Terminal Server	Terminal server maintenance documentation — available on CD and hard copy from the vendor.
Ethernet switch	HP ProCurve Series 2500 Switches Management and Configuration Guide (5969-2354)
Paradyne Modem	<p>Paradyne documentation — available from the vendor at http://www.paradyne.com. Includes the following:</p> <ul style="list-style-type: none"> Comsphere 3900 Series Modems, Models 3910 and 3911, Point-To-Point/Multipoint Installation and Operation Manual Comsphere 3800 Series Modems, Models 3810, 3811, and 3820, User's Guide
ARCA-DACS™	<p>ARCA-DACS documentation — general information available at www.zhone.com. The following documentation ships with the product:</p> <ul style="list-style-type: none"> Configuration Management Tool, SECTOR 300 & ARCA-DACS 100, Release 2.5.2, User's Guide CMT for Windows NT, Release 2.5.2, Release Notes
TRAK 9100	Technical Manual, Model 9100, Modular Frequency/Time System , March 2002, CD-ROM

This page intentionally left blank.

Managing the LAN Switch

This chapter describes how to manage the LAN switch using CiscoWorks2000, a network management application that includes CiscoView Device Manager and Resource Manager Essentials (RME).

The CiscoWorks applications reside on the Ethernet Switch Management Server (ESMS) and work together as a LAN management solution.

This chapter describes how to use these applications in your Motorola® system and includes the following topics:

- "Managing Security Access" on page 1-2
- "Master Site System Diagram" on page 1-4
- "Accessing CiscoWorks2000" on page 1-5
- "Using CiscoView" on page 1-9
- "Using Resource Manager Essentials" on page 1-35
- "Displaying LAN Switch Alarms in HP OpenView" on page 1-66



CAUTION

Do not tamper with factory configuration settings for the ESMS. This includes software configuration, firmware release, password, and physical connections. Motorola has configured and connected this device to meet very specific performance requirements. Tampering with this device may result in unpredictable system performance or catastrophic failure. In the event you need to make configuration changes you must contact Motorola System Support Center (SSC) before attempting any configuration changes or software upgrades of network transport devices.



NOTE

To access CiscoWorks2000, you must use the Transport Network Management (TNM) client workstation.

Managing Security Access

CiscoWorks2000 uses two levels of access which are accordingly assigned to users. The access levels are:

- **Administrator user account (cwmgr):** A user with read/write access who can perform all the supported features delivered by CiscoWorks2000.
- **Help Desk user account (cwusr):** A user with view only access who can perform many tasks, but cannot perform some tasks that are limited to the cwmgr account.



NOTE

The passwords are confidential and provided by Motorola to approved users. Contact your Motorola support person for more information.

See Procedure 1-1, "How To View Account Permissions," on page 1-2 for information on viewing the user permissions.

Viewing Account Permissions

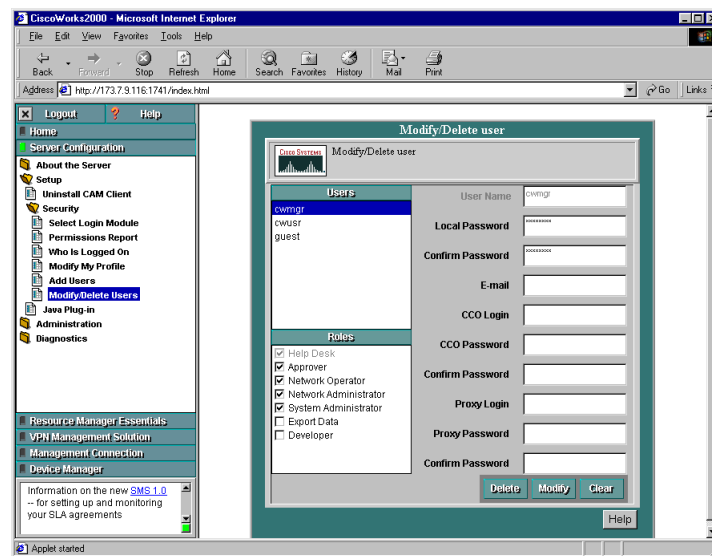
Procedure 1-1 describes how to view account permissions.

Procedure 1-1 How To View Account Permissions

- 1 Select **Server Configuration** in the navigation pane of the CiscoWorks2000 main window (Figure 1-6, "CiscoWorks2000 Login Manager Pane" on page 1-7).
- 2 Select **Setup**, select **Security**, and then select **Modify/Delete** users.

Result: The Modify/Delete User pane appears (Figure 1-1).

Figure 1-1 Modify/Delete User Pane



Procedure 1-1 How To View Account Permissions (Continued)

- 3
- In the Users column, click the user **cwmgr**.
Result: The Roles area shows the permissions for this user: Approver, Network Operator, Network Administrator, and System Administrator.

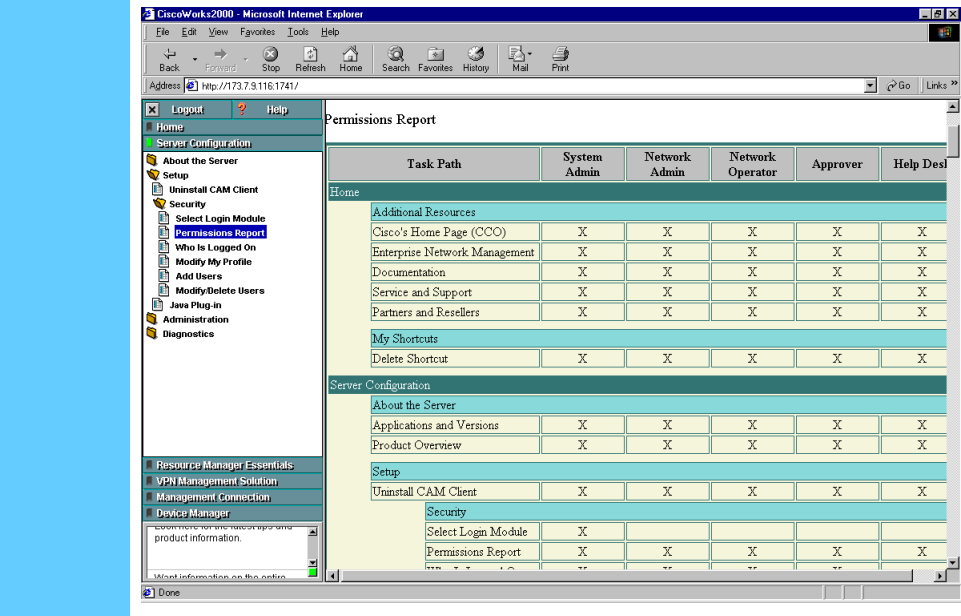


NOTE

If you had selected **cwusr**, the Roles area would show Help Desk only.

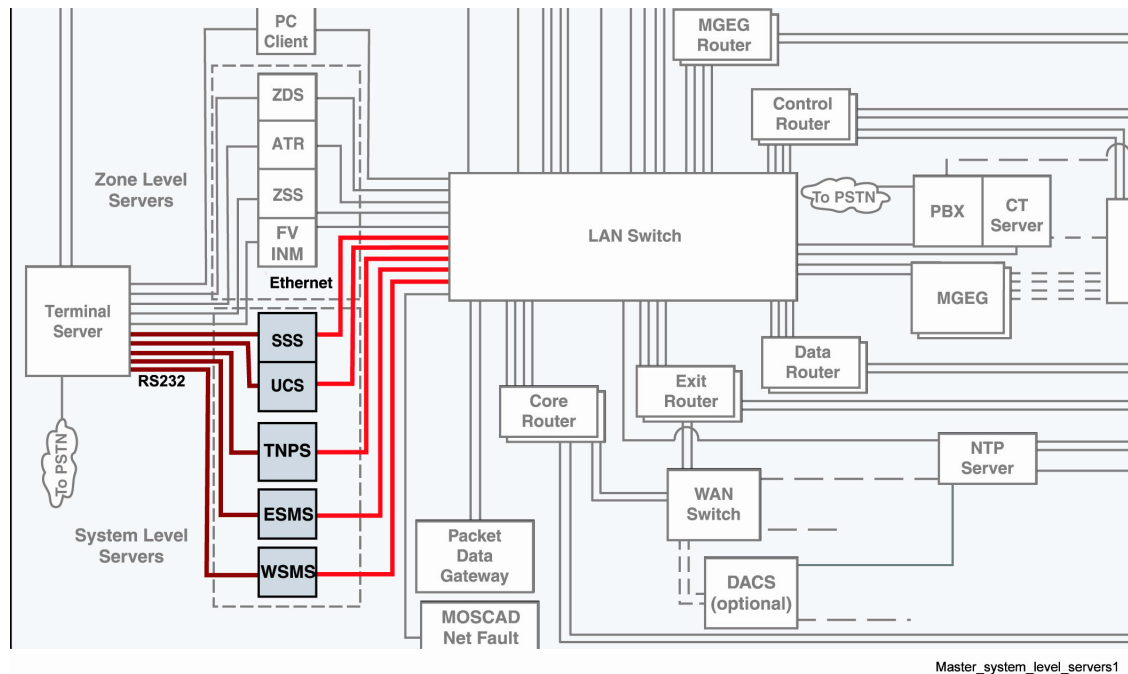
- 4
- To determine the exact permissions for the user, select **Security** and then select **Permissions Report**.
Result: The Permissions Report pane appears (Figure 1-2). This pane shows a detailed table of all of the permissions allowed to each user.

Figure 1-2 Permissions Report Pane



Master Site System Diagram

Figure 1-3 shows how the ESMS, where CiscoWorks2000 resides, fits into the system Master Site.

Figure 1-3 System Diagram Example

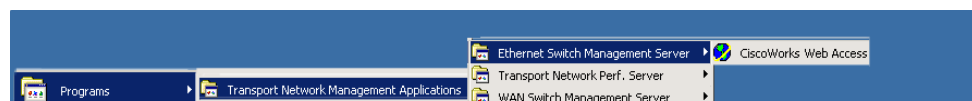
Accessing CiscoWorks2000

This section describes how to access CiscoWorks2000.

Access Points for CiscoWorks2000

You can access CiscoWorks2000 from two places on the TNM client workstation:

- From the Start menu, select **Programs**, select **Transport Network Management Applications**, select **Ethernet Switch Management Server**, and then select **CiscoWorks Web Access** (Figure 1-4).

Figure 1-4 Transport Network Management Applications Menu

- From the TNM client desktop, double-click the **CiscoWorks Web Access** icon (Figure 1-5).

Figure 1-5 Desktop Icon



NOTE

To bookmark the site, the CiscoWorks2000 URL is **<http://10.0.0.17:1741/index.html>**.

Launching CiscoWorks2000

"Launching CiscoWorks2000" on page 1-6 describes how to launch CiscoWorks2000. See Volume 9, *Network Transport Applications Installation and Configuration*.

**NOTE**

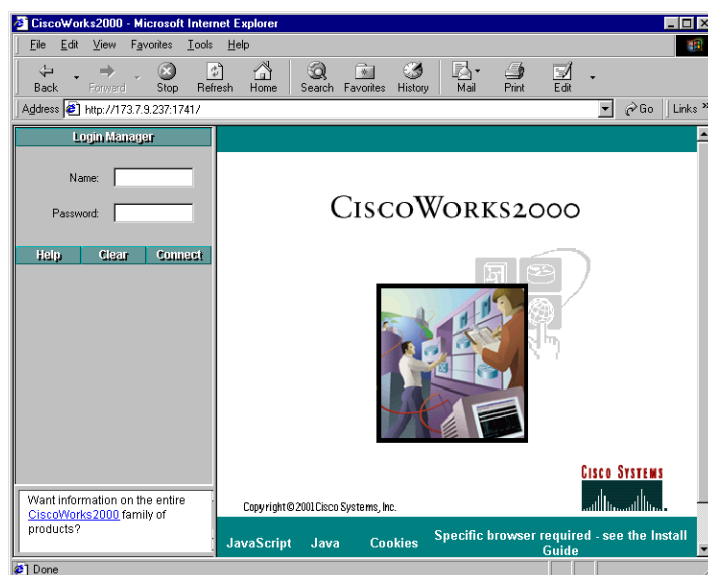
If you have problems accessing these applications, see Volume 9, *Network Transport Applications Installation and Configuration* for the steps to configure CiscoWorks2000 and CiscoView.

Procedure 1-2 How to Launch CiscoWorks2000

- 1 From the TNM client desktop, double-click the **CiscoWorks Web Access** icon (Figure 1-5).

Result: The CiscoWorks2000 Login Manager pane appears (Figure 1-6).

Figure 1-6 CiscoWorks2000 Login Manager Pane



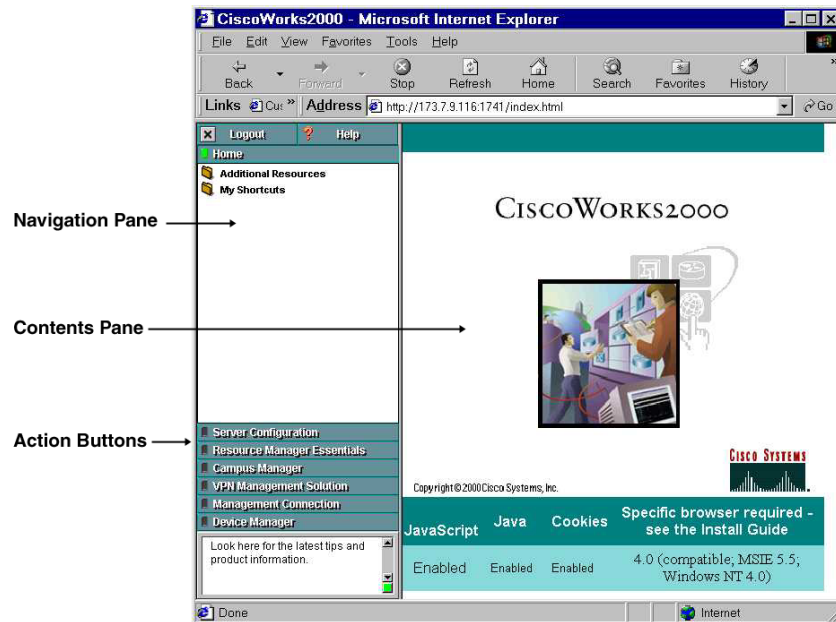
- 2 In the Name field, type **cwmgr** or **cwusr**. In the Password field, type the password.

Procedure 1-2 How to Launch CiscoWorks2000 (Continued)

3 Click **Connect**.

Result: The navigation and contents pane appear (Figure 1-7).

Figure 1-7 CiscoWorks2000 Main Window - Navigation Pane



4 Depending on the task, click one of the following action buttons:

- **Logout** — returns the browser to the Login Manager pane.
- **Help** — accesses the online help in a separate browser window. Information about the CiscoWorks2000 interface is covered in the CiscoWorks2000 Help topic, “Interacting with the CiscoWorks2000 Desktop.”
- **Server Configuration** — accesses applications and tools for setting up, administering, and diagnosing the CiscoWorks2000 server.
- **Resource Manager Essentials** — accesses Resource Manager Essentials (Essentials) suite, which is part of the CiscoWorks2000 family of products.
- **Device Management** — accesses applications used for device management, such as CiscoView. (CiscoView manages the LAN switches and Multilayer Switch Feature Card (MSFC) routers.)



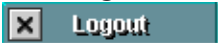

NOTE

You do not use all of the CiscoWorks features (for example, the Home, VPN Management Solution, and Management Connection buttons are not used in the Motorola system). You also cannot use any menu option that mentions CCO, which refers to the online Cisco Service Center, because your system is a closed system.

Exiting CiscoWorks2000

Procedure 1-3 describes how to exit CiscoWorks2000.

Procedure 1-3 How to Exit CiscoWorks2000

1	<p>Click Logout</p>  <p>in the CiscoWorks2000 main window.</p> <p>Result: A message appears to inform you that the login session was terminated.</p>
2	<p>Click OK to dismiss the message.</p> <p>Result: The Login Manager pane appears (Figure 1-6, "CiscoWorks2000 Login Manager Pane" on page 1-7).</p>
3	<p>Click the Close button on the browser window to exit from CiscoWorks2000.</p> 

Using CiscoView

CiscoView is a Web-based device management tool that provides real-time views of networked LAN switches. The views provide a continuously updated representation of device configuration and performance conditions. Simultaneous views are available for multiple sessions so that multiple users can simultaneously access the tool.

CiscoView manages the LAN switches and Multilayer Switch Feature Card (MSFC) routers.

The following procedures are performed on the LAN switch using CiscoView Device Manager:

- "Viewing the System Time" on page 1-15
- "Displaying VLAN Members" on page 1-17
- "Monitoring the Performance of Ethernet Ports" on page 1-19
- "Creating and Monitoring System Logs" on page 1-22
- "Monitoring the Performance of a LAN Switch" on page 1-27
- "Monitoring the Performance of MSFC Routers" on page 1-31
- "Using CiscoView for Fault Management" on page 1-33

CiscoView Features

Use CiscoView to do the following:

- View a physical representation of front and back device panels, including component (interface, card, power supply) status.
- Display the status of a device — when monitoring the status of a device, status colors indicate status as follows:
 - Green light — shows a normal and active status.
 - Red light — shows an abnormal status.
 - Yellow light — indicates a standby status.
 - Brown port — indicates an inactive mode.
- Monitor real-time statistics for interfaces, resource utilization, and device performance. Monitoring capabilities display performance and other statistics.



NOTE

CiscoView has some capabilities to reset the LAN switch, back up and restore the switch, and download software to the switch, but since Resource Manager Essential (RME) has more advanced features to schedule these tasks and to view historical data, this CiscoView functionality is not discussed in this document.

Embedded CiscoView

Table 1-1 compares the features of Embedded CiscoView (which resides on the WAN switch and contains a subset of the features that CiscoView contains) to the features of CiscoView.

Table 1-1 Embedded CiscoView Features

Feature	Embedded CiscoView	CiscoView
Needs CiscoWorks	no	yes
Runs on PNM Client	yes	no
Handles Multi-layer Switch Feature Card (MSFC) Router	no	yes
Displays Performance	no	yes
One dedicated for each device	yes	no

Accessing CiscoView and CiscoView Commands

Procedure 1-4 describes how to access CiscoView and the CiscoView commands that are available from a pop-up menu.

Procedure 1-4 How to Access CiscoView and CiscoView Commands

- 1 Select **Device Manager** in the navigation pane of the CiscoWorks2000 main window (Figure 1-7).
- 2 Click **CiscoView**.
Result: The CiscoView in CiscoWorks2000 main window appears (Figure 1-8).

Figure 1-8 CiscoView Main Window



- 3 From the **Select Device** list, select an IP address from the list. If a desired address is not in the list, type in the IP address.
 - <IP address of the LAN switch>,
 - <IP address of the LAN switch router 1>
 - <IP address of the LAN switch router 2>



NOTE

The IP address varies based on your system. IP addresses are created during the installation and configuration process using RME.

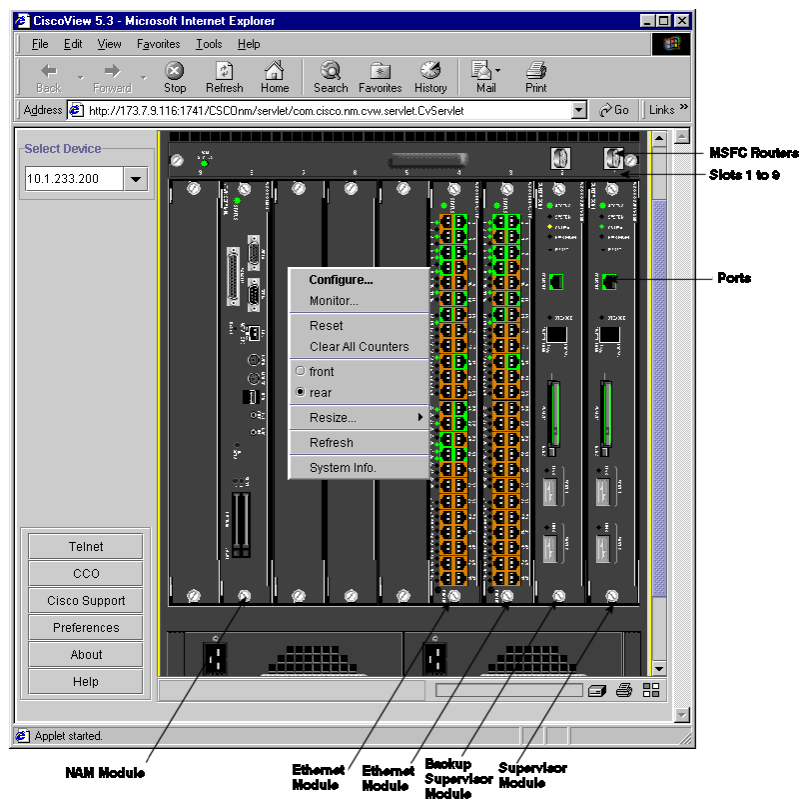
Result: The back plane of the selected device appears.

Procedure 1-4 How to Access CiscoView and CiscoView Commands (Continued)

- 4** Do one of the following to access the pop-up menu options for the device that you selected.
1. Click directly on a port, device, power supply, module, submodule, or CPU in the device display.
 2. Hold down the right mouse button on that item, and select an option from the pop-up menu display.

Result: Figure 1-9 shows the a pop-up menu on the view of the LAN switch, along with other labeled elements.

Figure 1-9 Pop-Up Menu



Procedure 1-4 How to Access CiscoView and CiscoView Commands (Continued)**5**

Select one of the following menu options:

**NOTE**

The pop-up menu contains different options depending on where you select to view.

- **Configure** — opens the Configure dialog box for the device, card, port on the card, or power supply.
- **Monitor** — opens the Monitor dialog box for a card or ports.
- **Reset** — resets the selected device or port.
- **Clear All Counters** — clears the port and device counters (device-specific command).
- **Front** — displays the front view of the device.
- **Rear** — displays the rear view of the device.
- **Resize** — changes the size of the device view.
- **Refresh** — refreshes the device view.
- **System Info.** — displays the System Information dialog box that contains the name, description, and other information about the device.

Viewing System Information

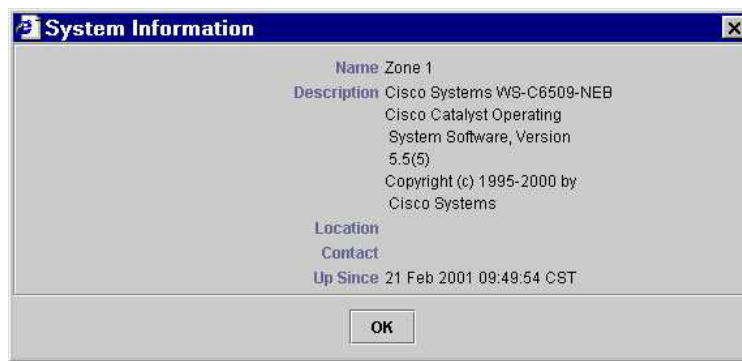
Procedure 1-5 describes how to view system information. This information is important for troubleshooting; it is used to verify if you have the correct software version after performing a software upgrade.

Procedure 1-5 How to View the System Information

- 1 Right-click on an empty card slot in the device view and select **System Info** from the pop-up menu.

Result: The System Information dialog box appears (Figure 1-10).

Figure 1-10 System Information Dialog Box



- 2 Verify that the Catalyst Operating System (COS) software version and other information is correct.

Viewing the System Time

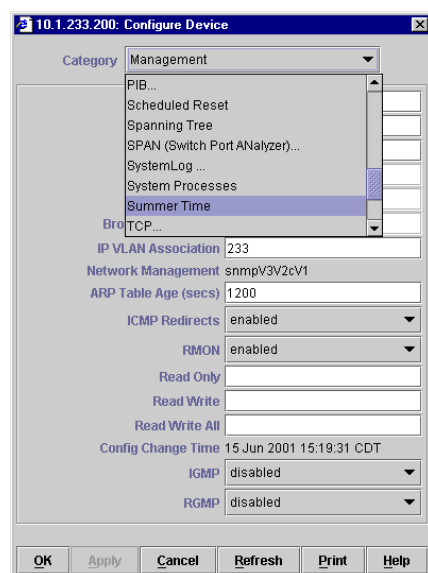
Procedure 1-6 describes how to use the System Time dialog box to see the time on the LAN switch. A correct system time helps you determine what time a problem occurred on the switch.

Procedure 1-6 How to View the System Time

- 1 Right-click on an empty card slot in the device view and select **Configure**.

Result: The Configure Device dialog box appears (Figure 1-11).

Figure 1-11 Configure Device Dialog Box



Procedure 1-6 How to View the System Time (Continued)

2 From the **Category** menu, select **Summer Time**.

Result: The Summer Time dialog box appears (Figure 1-12). (Summer Time indicates that daylight savings time is configured.)

Figure 1-12 Summer Time Dialog Box

10.1.233.200: Configure Device

Category Summer Time

Country Location

Summer Time Status Disable

Summer Time Offset 0

Current Date and Time (YYYY-MM-DD HH:MM)

2001 Jun 16 11 : 10

Summer Time Recurring Start

1 Sun Jan 0 0

Summer Time Recurring End

1 Sun Jan 0 0

OK Apply Cancel Refresh Print Help

3 Look at the Current Date and Time fields to see the current System Time settings. You can click **Refresh** to refresh the time.

Displaying VLAN Members

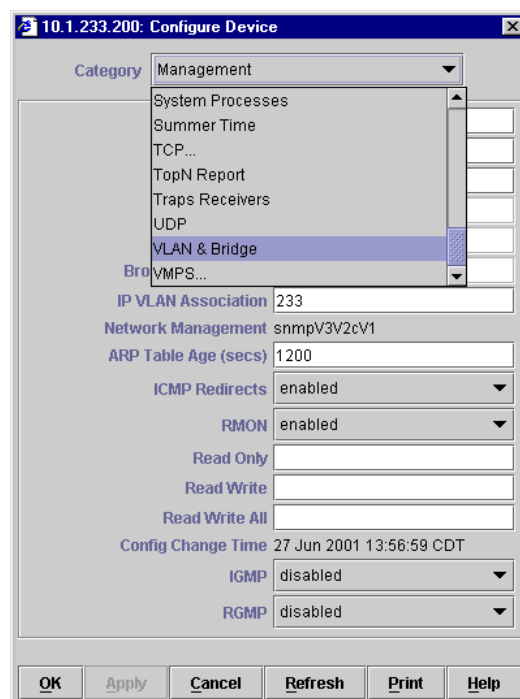
Procedure 1-7 describes how to display Virtual LAN (VLAN) members. Ports on the LAN switch create a VLAN, allowing devices connected to the LAN switch to communicate with each other. This procedure allows you to view the configuration of the VLAN to see which ports belong to that VLAN. If a port changes color (for example, changes to red), you can determine how the malfunctioning port impacts network performance.

Procedure 1-7 How to Display VLAN Members

- 1 Right-click on an empty card slot in the device view and select **Configure**.

Result: The Configure Device dialog box appears (Figure 1-13).

Figure 1-13 Configure Device Dialog Box

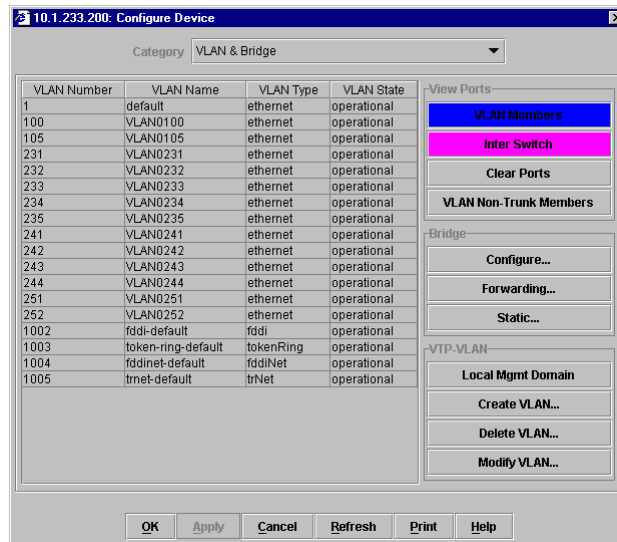


Procedure 1-7 How to Display VLAN Members (Continued)

2 From the **Category** list, select **VLAN & Bridge**.

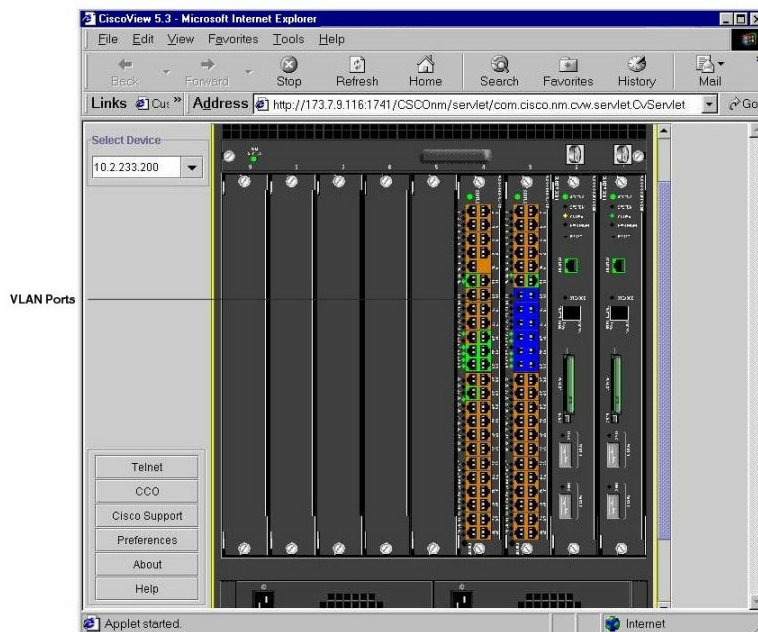
Result: The VLAN & Bridge Category appears (Figure 1-14).

Figure 1-14 VLAN & Bridge Category



Procedure 1-7 How to Display VLAN Members (Continued)

- 3** In the **VLAN Number** column, select a VLAN and click the blue **VLAN Members** button.
- Result:** A CiscoView message dialog displays the total number of members of the VLAN.
- 4** Click **OK**.
- Result:** In the CiscoView main window, ports that belong to that VLAN are marked blue (Figure 1-15).

Figure 1-15 VLAN Ports

Monitoring the Performance of Ethernet Ports

Procedure 1-8 describes how to monitor the performance of the Ethernet ports. You can monitor utilization, status, statistics, errors, and discards on an Ethernet port.

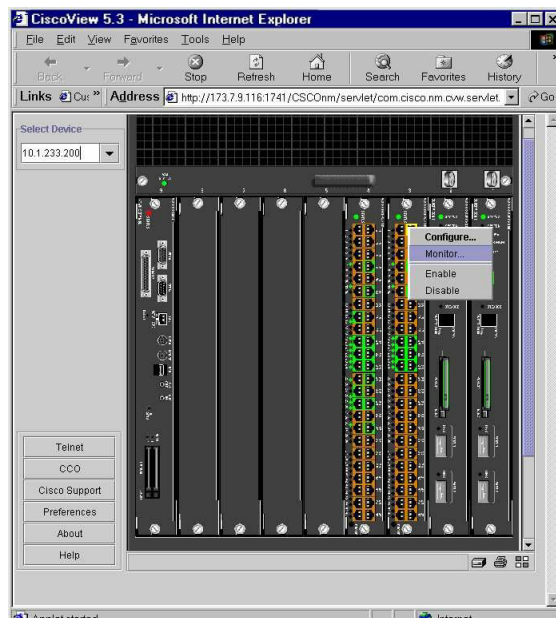
**IMPORTANT**

Only perform this procedure in a troubleshooting situation. Do not monitor more than 30 minutes at a time and stop the monitoring when completed.

Procedure 1-8 How to Monitor the Performance of Ethernet Ports

- 1 Right-click an Ethernet port and select **Monitor** (Figure 1-16).

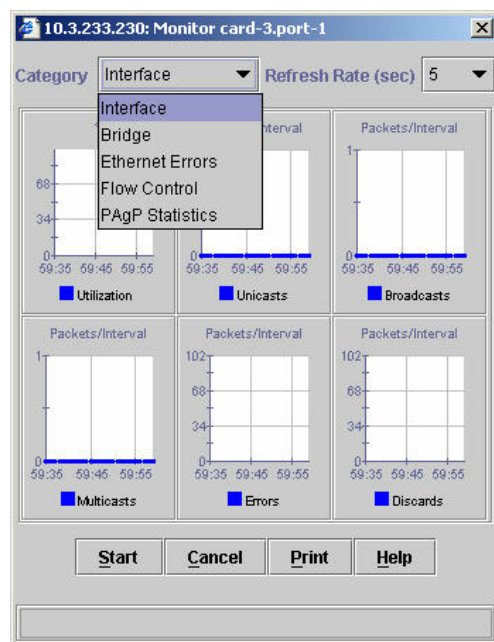
Figure 1-16 Ethernet Ports



Result: The Monitor Card dialog box appears (Figure 1-17).

Procedure 1-8 How to Monitor the Performance of Ethernet Ports (Continued)**2**Click the **Category** list and select an option to monitor (Figure 1-17).

- Select **Interface** to monitor port interface information.
- Select **Ethernet Errors** to monitor activity on an Ethernet port.

Figure 1-17 Monitor Card Dialog Box

Procedure 1-8 How to Monitor the Performance of Ethernet Ports (Continued)

3 To begin monitoring, select the **Refresh Rate**, if necessary, and then click **Start**.

Result: The button changes to **Stop**.

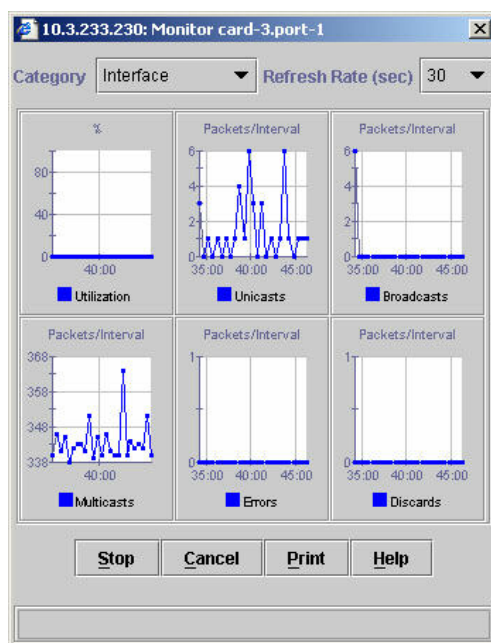
**NOTE**

For information about the type of information presented in the dialog box, click **Help**.

4 When you are finished monitoring, click **Stop**. Do not monitor more than 30 minutes at a time.

Result: The performance data collection stops (Figure 1-18).

Figure 1-18 Monitor Card Dialog Box (showing example data)



Creating and Monitoring System Logs

This section describes how to create and monitor System Logs. The System Log provides access to important messages or activities logged in the LAN switch. You could telnet to the switch for this information, but using CiscoView provides a safer access point.

Log files are similar to the UNIX system log and are used for the same purpose as an SNMP trap. The key difference is that this is the Cisco proprietary log and the information does not propagate to HP OpenView.

Creating System Logs

Procedure 1-9 describes how to create System Logs. By default, the system log is not enabled. If you want to view messages or activities that affect the LAN switch, you must create a System Log.



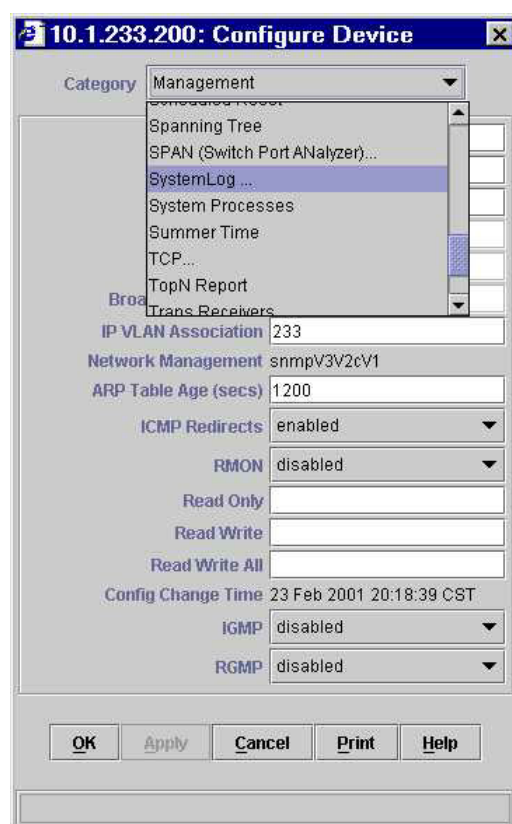
CAUTION

Creating a system log may impact network performance. Be sure to disable the System Log immediately when you are done troubleshooting.

Procedure 1-9 How to Create System Logs

- 1 Right-click on an empty card slot in the device view and select **Configure**.
Result: The Configure Device dialog box appears (Figure 1-19).

Figure 1-19 Configure Device Dialog Box

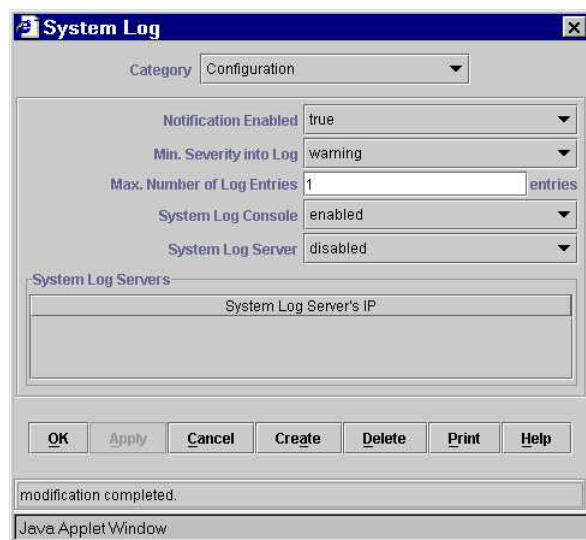


Procedure 1-9 How to Create System Logs (Continued)

- 2** From the **Category** menu, select **System Log**.

Result: The System Log dialog box appears (Figure 1-24)

Figure 1-20 System Log Dialog Box



- 3** In the System Log dialog box (Figure 1-24), click **Create**.

Result: The Row Creation dialog box appears (Figure 1-21).

Figure 1-21 Row Creation Dialog Box



Procedure 1-9 How to Create System Logs (Continued)

4 In the Host box, type the <ESMS IP Address> and click **OK**.

Result: The System Log dialog box reappears (Figure 1-22).

Figure 1-22 System Log Dialog Box

5 In the Max. Number of Log Entries field, enter the maximum number of log entries (for example, 100).

6 From the System Log Server list, select **enabled**.



NOTE

Once you enable the System Log, you can use the RME) Syslog Analysis feature for reports. (This feature is not covered in this documentation; see the online **CiscoWorks2000 User Manual** for more information. Click Help (Figure 1-23) on the CiscoWorks2000 main window to access online manual.)

Figure 1-23 Help Button



7 Click **Apply**. The system log is now created.

Monitoring a System Log

Procedure 1-10 describes how to monitor the System Log, using the following guidelines:

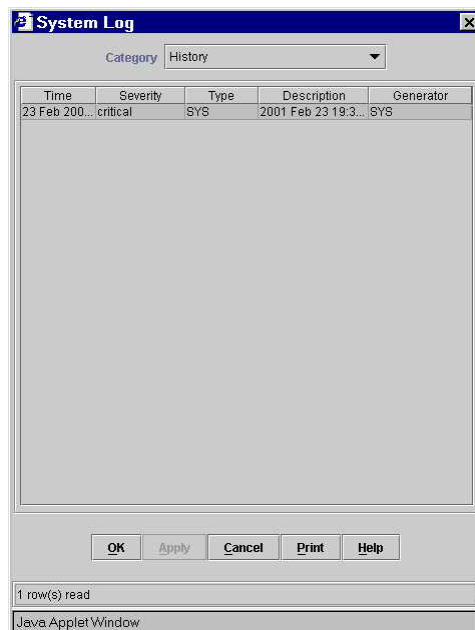
- You can view different types of logs (for example; configuration changes, unusual login attempts, the reset count on a switch, or memory failures).
- You can view key information such as the time the log was received, the severity of the log, and the type of log.

Procedure 1-10 How to Monitor the System Log

- 1 In the System Log dialog box (Figure 1-22), from the Category list, select **History**.

Result: The System Log dialog box updates to show the history (Figure 1-24).

Figure 1-24 System Log Dialog Box - History



Disabling the System Log

Procedure 1-11 describes how to disable the System Log after you are done with your troubleshooting.



IMPORTANT

You must disable the System Log immediately after troubleshooting to avoid impacting system performance.

Procedure 1-11 How to Disable the System Log

- 1 From the Category list, select **Configuration**.
Result: The System Log appears (Figure 1-25).

Figure 1-25 System Log Dialog Box

- 2 Change the following fields to **disabled**.
 - System Log Console
 - System Log Server
- 3 Click **Apply**.

Monitoring the Performance of a LAN Switch

This section provides an example of how to monitor the performance of the LAN switch using Simple Network Management Protocol (SNMP). Devices send SNMP messages that are used for monitoring the device.

Procedure 1-12 provides an example of how to display CPU utilization information over three different time periods (5 seconds, 1 minute, and 5 minutes). You could also view different performance categories, for example, SNMP Traffic.

**IMPORTANT**

Only perform this procedure in a troubleshooting situation. Do not monitor more than 30 minutes at a time and stop the monitoring when completed.

Procedure 1-12 How to Monitor the Performance of the LAN Switch

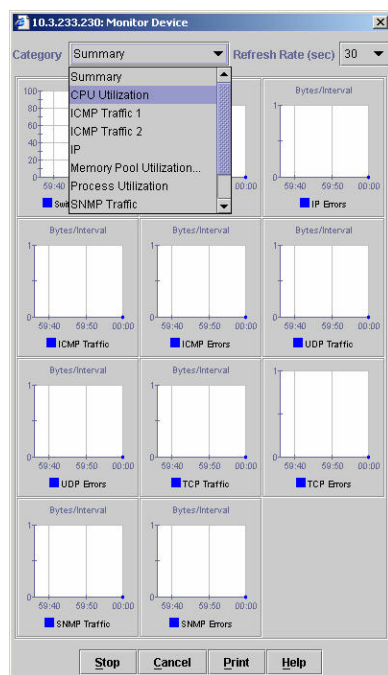
- 1 Right-click on an **empty** card slot in the device view and select **Monitor** from the pop-up menu.

**NOTE**

To perform this procedure correctly, you must select an empty card slot, which allows you to choose menu options for the LAN switch as a whole.

Result: The Monitor Device dialog box appears (Figure 1-26).

Figure 1-26 Monitor Device Dialog Box

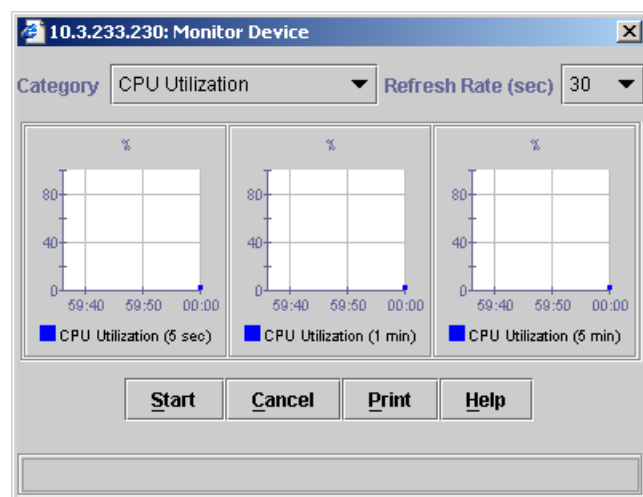


Procedure 1-12 How to Monitor the Performance of the LAN Switch (Continued)

2 Click the **Category** list and select **CPU Utilization**.

Result: The CPU Utilization dialog box appears displaying the CPU Utilization (Figure 1-27).

Figure 1-27 CPU Utilization Dialog Box



Procedure 1-12 How to Monitor the Performance of the LAN Switch (Continued)

3 To begin monitoring, select the **Refresh Rate**, if necessary, and then click **Start**.

Result: The button changes to **Stop**.

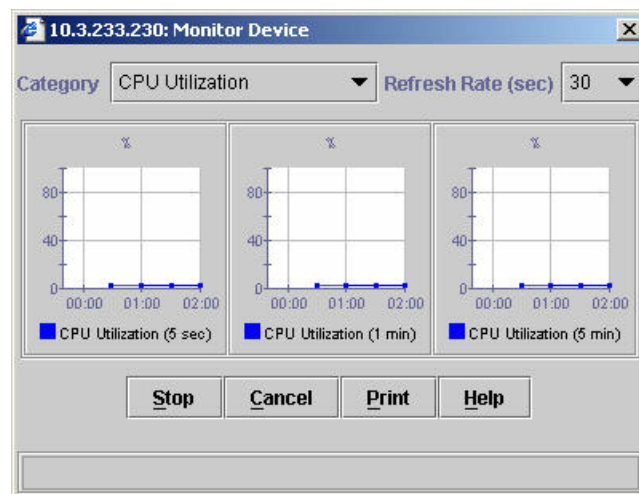
**NOTE**

For information about the type of information presented in the dialog box, click **Help**.

4 When you are finished monitoring, click **Stop**. Do not monitor more than 30 minutes at a time.

Result: The dialog box shows the new data (Figure 1-28).

Figure 1-28 CPU Utilization Dialog Box (showing example data)



Monitoring the Performance of MSFC Routers

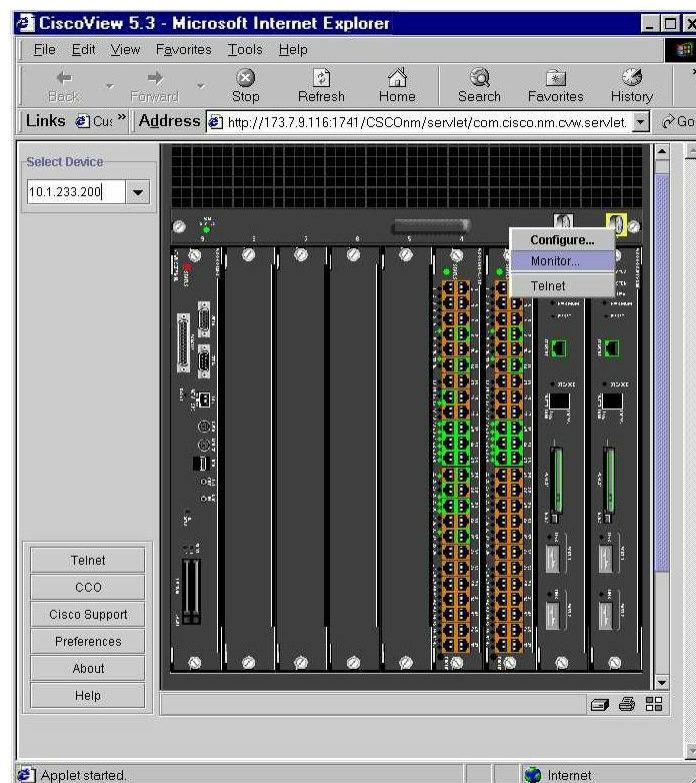
Procedure 1-13 describes how to monitor Multi-layer Switch Feature Card (MSFC) routers. You can view traffic patterns for the device, gauge CPU and memory utilization, and view SNMP traffic.

Procedure 1-13 How to Monitor the Performance of MSFC Routers

- 1 Right-click on the MSFC router icon.

Result: A pop-up menu appears (Figure 1-29).

Figure 1-29 MSFC Router Pop-up Menu

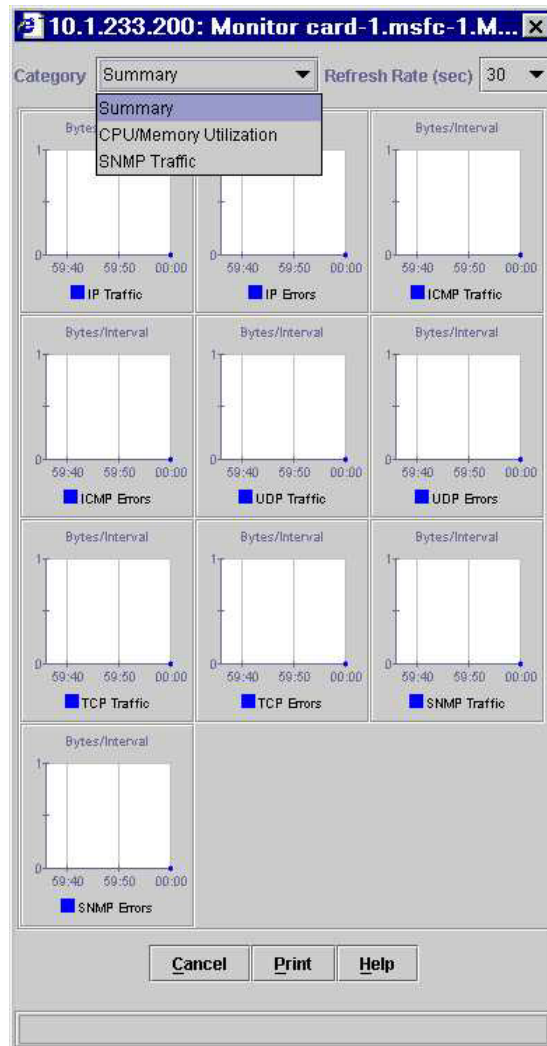


Procedure 1-13 How to Monitor the Performance of MSFC Routers (Continued)

2 Select **Monitor**.

Result: The Monitor Card dialog box appears (Figure 1-30).

Figure 1-30 Monitor Card Dialog Box



Procedure 1-13 How to Monitor the Performance of MSFC Routers (Continued)**3**

From the Category list, select one of the following:

- **Summary** — the Summary Monitoring dialog box displays general traffic graphs for the device.
- **CPU/Memory Utilization** — the CPU/Memory Utilization dialog box displays gauges of CPU and memory usage for the device.
- **SNMP Traffic** — the SNMP Traffic dialog box displays graphs of SNMP traffic on the device.

**NOTE**

If you need information about the type of information presented in each Monitor Card dialog box, click **Help** for help on the dialog boxes.

Using CiscoView for Fault Management

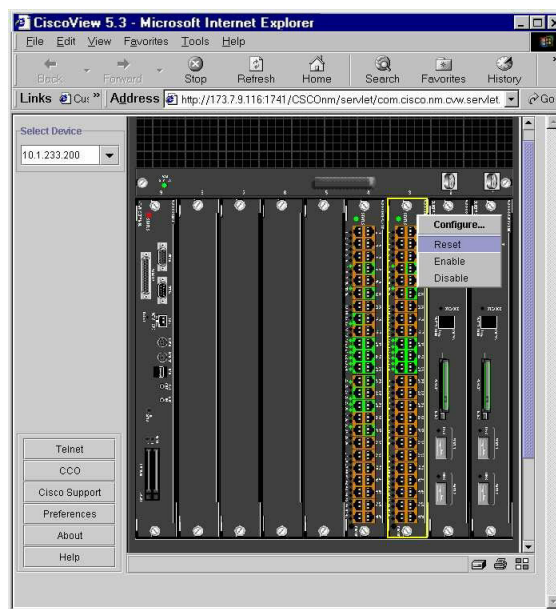
Procedure 1-14 describes how to reset the Ethernet Module for troubleshooting purposes. You can reset cards and ports on the card.

**CAUTION**

Only reset the Ethernet Module on the LAN switch after contacting the Motorola System Support Center and determining that this is the appropriate corrective action. Resetting this module will impact the system. The severity of the impact depends on the devices connected to the module, such as servers, client PCs, and routers.

Procedure 1-14 How to Reset the Ethernet Module

- 1 Right-click on an Ethernet module and select **Reset** to reset the module (Figure 1-31).

Figure 1-31 Ethernet Module

Result: The Are you sure? dialog box appears.

- 2 Click **Yes** to confirm.

Result: The module is reset.

Using Resource Manager Essentials

Resource Manager Essentials (RME) is a suite of Web-based applications that manage the LAN switches and the MSFC router cards on the LAN switch.



NOTE

See "Resource Manager Essentials Applications" on page 1-37 for the complete list of applications.

RME Features

RME is an enterprise solution to network management. This suite of Web-based network management tools enables administrators to collect the monitoring, fault, and availability information needed to track devices critical to the network.

Overview of Procedures

Table 1-2 provides an overview of RME procedures.

Table 1-2 Overview of RME Procedures

Procedure	Where the procedure is located
Back up the LAN switch software and configuration.	See "Backing Up the LAN Switch Software and Configuration" on page 1-42.
Restore the LAN switch configuration.	See "Restoring the LAN Switch Software and Configuration" on page 1-42.
Transfer software to and from the LAN switch.	See "Transferring New Software to the LAN Switch" on page 1-49.
Check device configuration and software changes.	See "Checking Device Configuration Changes and CiscoWorks2000 Users Who Made Changes" on page 1-58.

Accessing Resource Manager Essentials

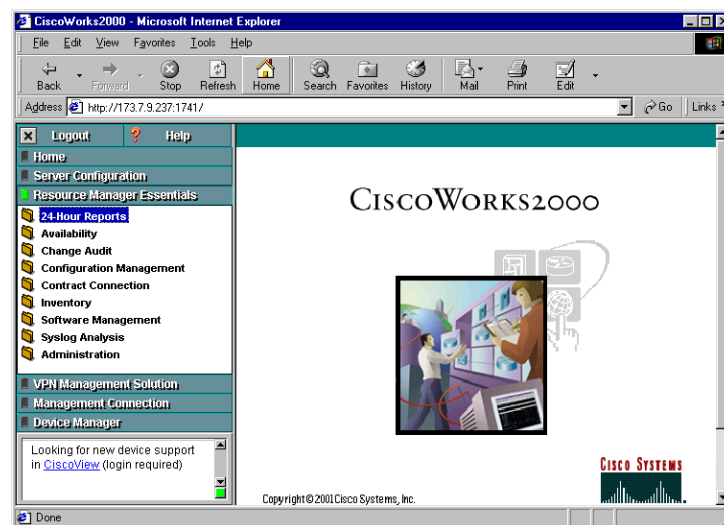
Procedure 1-15 describes how to access RME.

Procedure 1-15 How to Access RME

- 1 Select **Resource Manager Essentials** in the navigation pane of the CiscoWorks2000 main window.

Result: The Resource Manager Essentials suite appears (Figure 1-32).

Figure 1-32 Resource Manager Essentials Suite



Resource Manager Essentials Applications

Table 1-3 lists and describes the applications that are part of the RME suite.

Table 1-3 RME Applications

Application Name	Purpose
24-Hour Reports	<ul style="list-style-type: none"> Tells you if the switch was available from present to the last 24 hours. Lets you know when the switch was reloaded and why. Provides real-time performance statistics on the device. (See the online <i>CiscoWorks2000 User Manual</i> for more information.)
Availability	<ul style="list-style-type: none"> Monitors the reachability and response time of user-selected devices on the network. Collects fault and performance information for routers and switches.
Change Audit	<ul style="list-style-type: none"> Views and searches a central repository of all network changes (for example, inventory and software management). Sets up periods of time to monitor network changes. Maintains the repository. Converts changes into SNMP traps and forwards them to your network management system.
Configuration Management	<ul style="list-style-type: none"> Backs up a copy of the switch and router configuration files. Searches the archive for configuration files based on criteria you specify. Creates custom reports for repetitive tasks. Groups configuration files and labels them as a set. Edits configuration files stored in configuration archive and downloads files to devices. Creates network show command sets. Assigns users to network show command sets. Defines and schedules batch reports that can be executed at any time you specify.
Contract Connection	Not used

Table 1-3 RME Applications (Continued)

Application Name	Purpose
Inventory	<ul style="list-style-type: none">• Imports devices from databases or files.• Adds, deletes, changes, and lists devices in your network inventory.• Schedules polling and collection to update your network inventory.• Displays reports and graphs of your hardware and software inventory, and creates inventory custom reports.• Checks and changes device attributes.• Allows other network management systems to manipulate RME devices.• Installs support for new devices and enhanced support for existing devices.
Software Management	<ul style="list-style-type: none">• Analyzes upgrade needs and performs upgrades for Cisco devices on your network.• Validates images with devices before initiating downloads, and defines and monitors the progress of scheduled jobs.
Syslog Analysis	<ul style="list-style-type: none">• Troubleshoots and tracks device problems.• Views summaries of real-time reports on events that are being logged to syslog on behalf of a router or switch.• Processes these messages to generate reports.• Configures automatic actions that occur when certain message types are received.
Administration	<ul style="list-style-type: none">• Provides links to RME administrator tasks. These tasks include setup and maintenance that might need to occur before an application is used. For example, you can set up the polling of a switch or compare configuration files at a specified time.

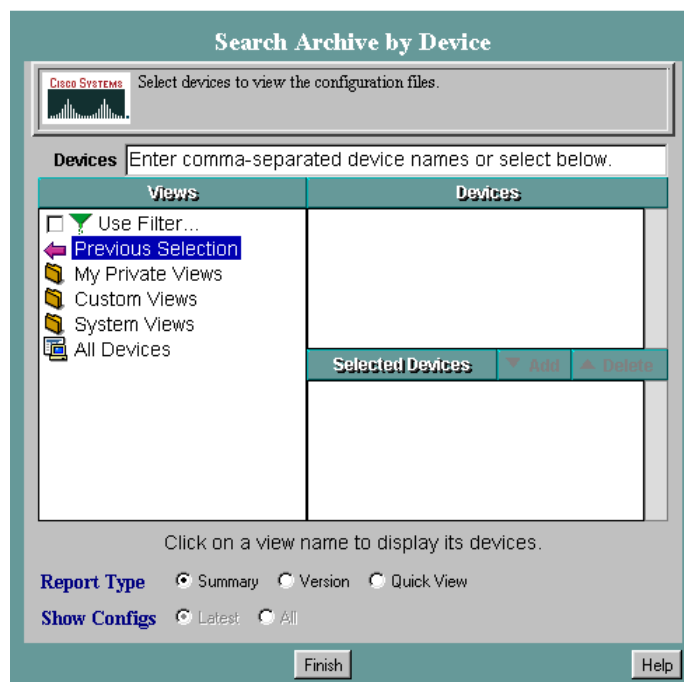
Viewing the LAN Switch Configuration

Procedure 1-16 describes how to view the LAN switch configuration.

Procedure 1-16 How to View the LAN Switch Configuration

- 1** Select **Resource Manager Essentials** in the navigation pane of the CiscoWorks2000 main window.
Result: The Resource Manager Essentials suite appears.
- 2** Select **Configuration Management** and select **Search Archive by Device**.
Result: The Search Archive by Device dialog box appears (Figure 1-33).

Figure 1-33 Search Archive by Device Dialog Box



Procedure 1-16 How to View the LAN Switch Configuration (Continued)

- 3** In the Views list, click **All Devices**. In the Devices list, select the LAN switch IP address whose configuration you want to view. Then click **Add**.

Result: The LAN switch IP address appears in the Selected Devices list (Figure 1-34).

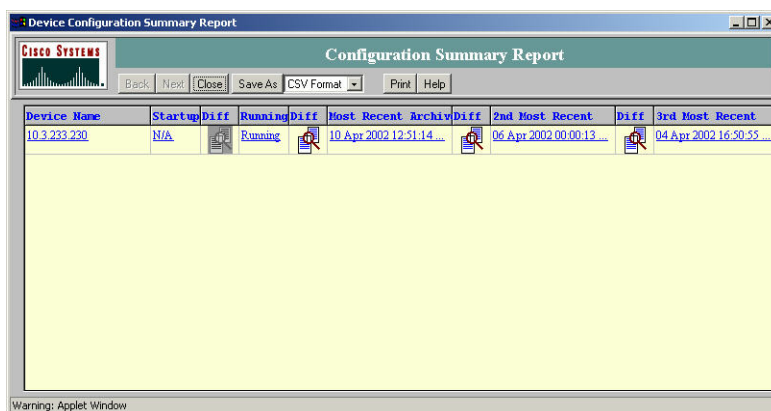
Figure 1-34 Selected Devices List



- 4** Click **Finish**.

Result: The Device Configuration Summary Report dialog box appears (Figure 1-35).

Figure 1-35 Device Configuration Summary Report Dialog Box

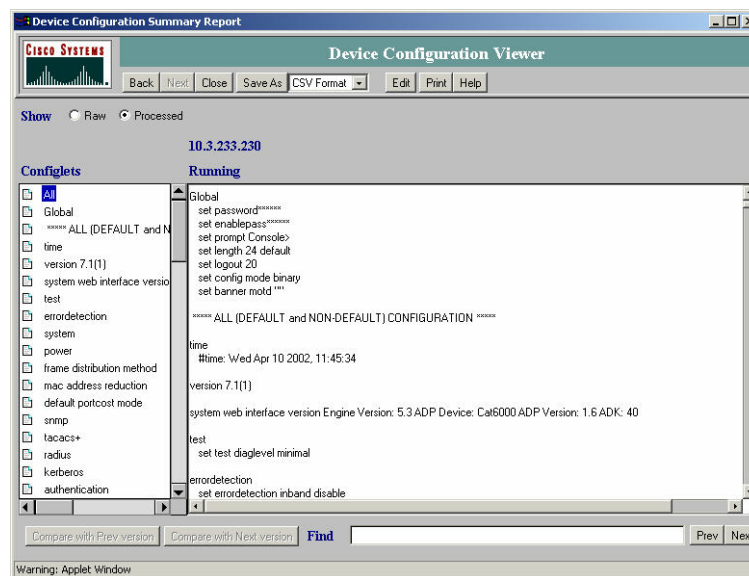


Procedure 1-16 How to View the LAN Switch Configuration (Continued)

5 Click **Running** to view the current configuration.

Result: The Device Configuration Viewer window appears (Figure 1-36).

Figure 1-36 Device Configuration Viewer Window



6 To view the critical configuration functions, select a Configlets option in the Configlets pane. The view in the Running pane changes to show that information. For example:

- **SNMP** displays SNMP configuration commands.
- **Global** displays global configuration commands.

Backup and Restore Guidelines

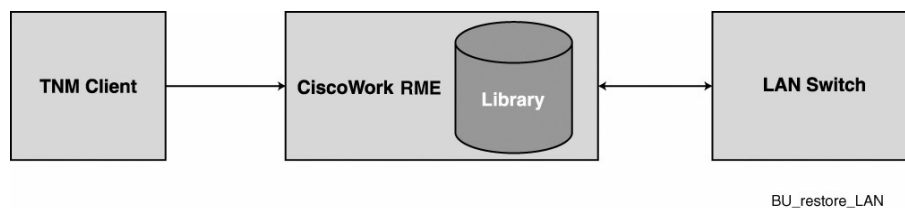
Table 1-4 lists the types and recommended frequency of LAN switch configuration files backups and restores.

Table 1-4 Recommended Frequency of Backups and Restores

Type of Backup/Restore	When performed
Backup after initial configuration	See Volume 9, <i>Network Transport Applications Installation and Configuration</i> .
Backup through automatic synchronization	Scheduled to synchronize every night, but only backs up if the configuration changes. See Volume 9, <i>Network Transport Applications Installation and Configuration</i> .
Restore	As needed

Figure 1-37 shows the backup and restore process for the LAN switch.

Figure 1-37 Backup and Restore LAN Switch Process Diagram



Backing Up the LAN Switch Software and Configuration

No other mechanism is provided for manual backup because a daily synchronization schedule is set up during the installation and configuration process. See Volume 9, *Network Transport Applications Installation and Configuration*.

Once this initial backup copy is added to the CiscoWorks library, you can push a copy to the switch at any time (see "Transferring New Software to the LAN Switch" on page 1-49).

Restoring the LAN Switch Software and Configuration

Procedure 1-17 describes how to restore an old configuration. You only restore the LAN switch software or configuration if there is a problem with new software, and you want to revert to a previous configuration.

**IMPORTANT**

You must contact Motorola System Support Center (SSC) before attempting this procedure as it may impact system performance.

Procedure 1-17 How to Restore an Old Configuration

- 1 Select **Resource Manager Essentials**, select **Configuration Management**, and select **Search Archive by Device**.

Result: The Search Archive by Device dialog box appears (Figure 1-38).

Figure 1-38 Search Archive by Device Dialog Box

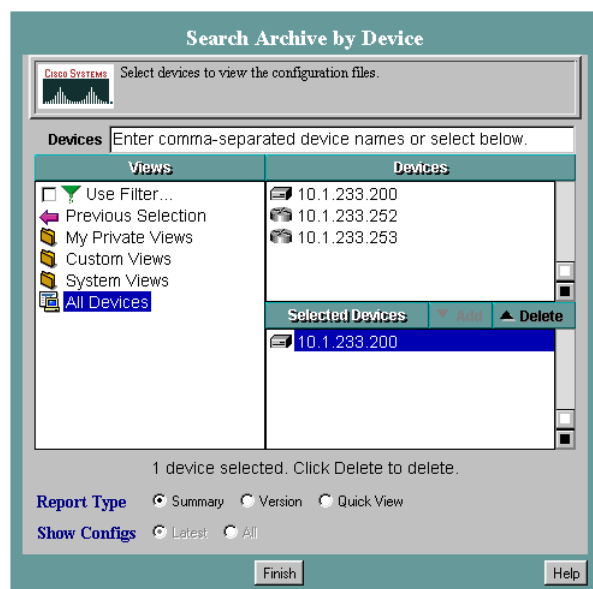


Procedure 1-17 How to Restore an Old Configuration (Continued)

- 2** In the Views list, click **All Devices**. In the Devices list, select the devices whose configurations you want to search. Then click **Add**.

Result: The devices appear in the Selected Devices list (Figure 1-39).

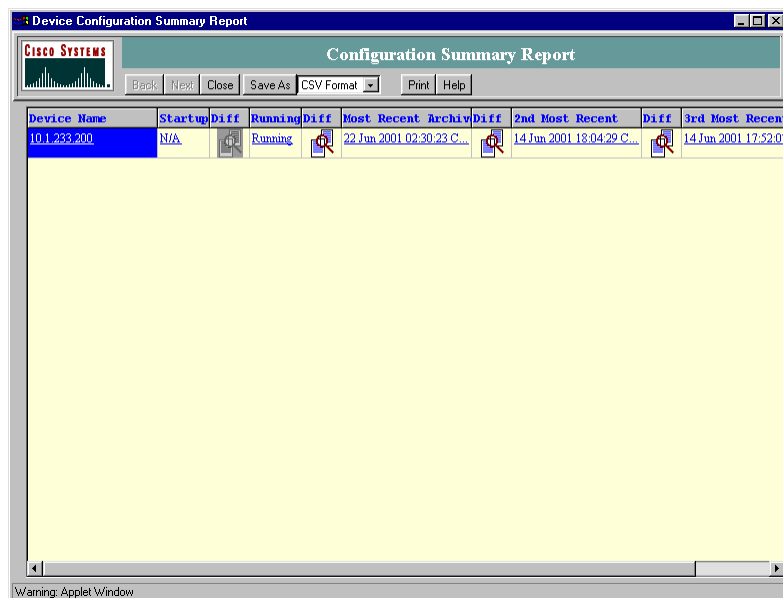
Figure 1-39 Selected Devices List



- 3** Click **Finish**.

Result: The Device Configuration Summary Report dialog box appears (Figure 1-40).

Figure 1-40 Device Configuration Summary Report Dialog Box

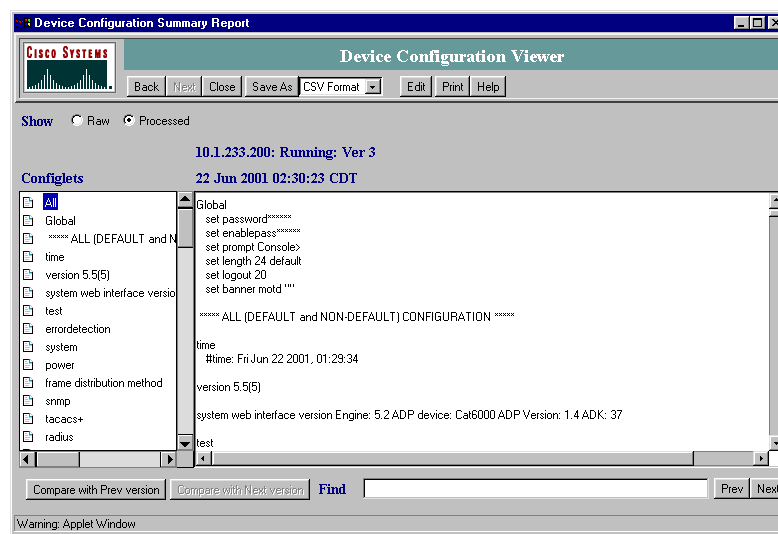


Procedure 1-17 How to Restore an Old Configuration (Continued)

- 4** Click the configuration file you want to transfer to the LAN switch (for example, Most Recent Archive).

Result: The configuration appears in the Device Configuration Viewer window (Figure 1-41).

Figure 1-41 Device Configuration Viewer Window

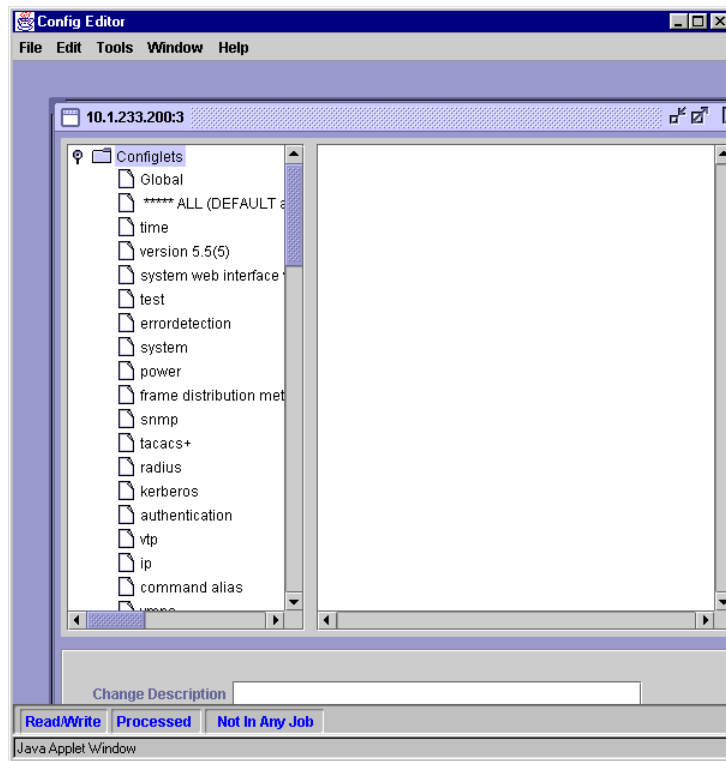


Procedure 1-17 How to Restore an Old Configuration (Continued)

- 5** Click **Edit** on the Device Configuration Viewer window.

Result: The Config Editor window appears (Figure 1-42) and a dialog box appears stating that the configuration will be locked.

Figure 1-42 Config Editor Window



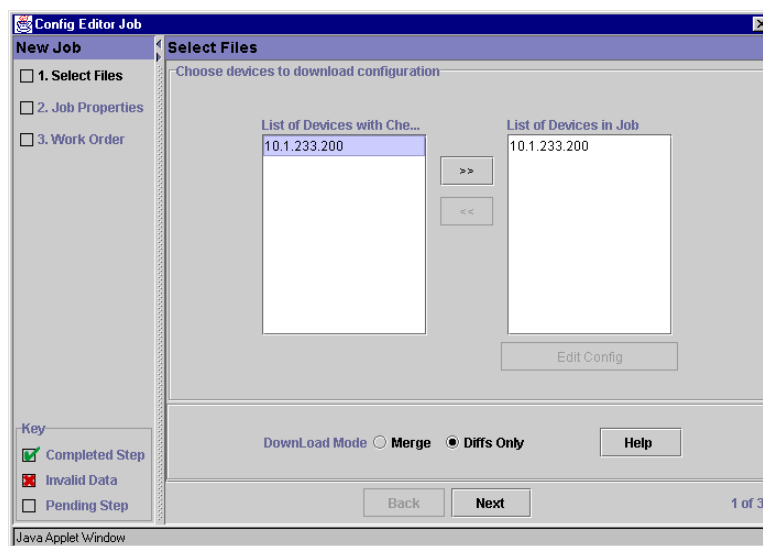
- 6** Click **OK** to dismiss the dialog box.

Procedure 1-17 How to Restore an Old Configuration (Continued)

7 From the File menu, select **Download**.

Result: The Config Editor Job wizard appears (Figure 1-43).

Figure 1-43 Config Editor Job Wizard



- The left pane lists the high-level tasks required to define the job. Each job has a corresponding dialog box that shows you the status of each task. The key at the bottom of the pane defines the task status indicators.
- The right pane contains the dialog boxes you use to define and schedule the job.

8 Select the devices on which to run the job from List of Devices and move them into **List of Devices in Job** by clicking the >> button.

**NOTE**

The current device (for which you have modified the configuration file) is selected by default.

Procedure 1-17 How to Restore an Old Configuration (Continued)

- 9** Select **Merge** to merge the complete file with the existing file in the configuration archive, or select **Diffs Only** to download only the commands that you have changed in the configuration file. If no differences exist between the files, the Diffs Only command does not execute.

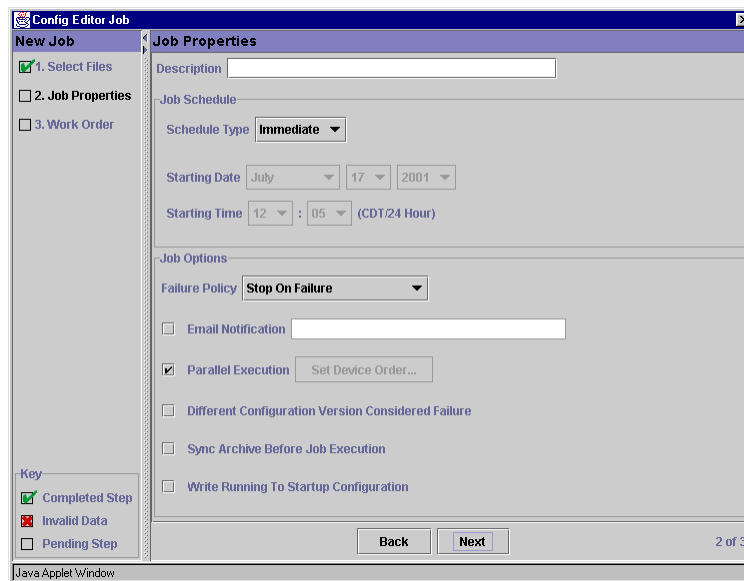
**NOTE**

If you select Diffs Only, the commands in the modified file are compared with the latest version in the configuration archive and the differences are displayed in the work order. If the configuration for the same device is then modified outside of CiscoWorks2000, another version is archived. That is, the latest version in the archive is changed. In such a case, when you review the work order later, a different set of commands might be displayed in the work order.

- 10** Click **Next**.

Result: The Job Properties dialog box appears (Figure 1-44).

Figure 1-44 Job Properties Dialog Box

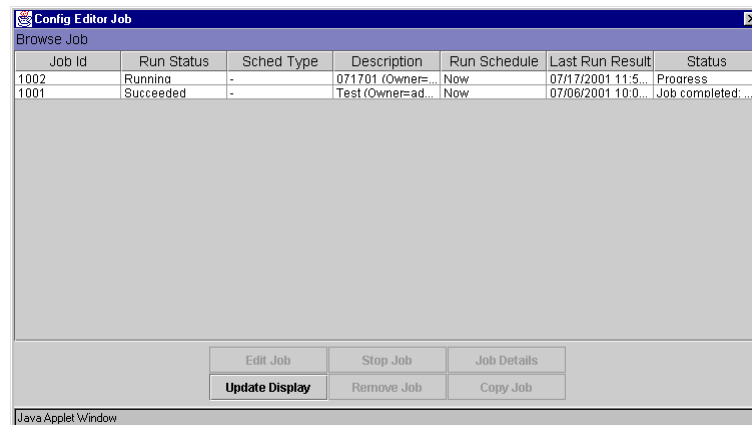


- 11** Enter the following information:

- In the Description box, type a name (whatever you like).
- For Schedule Type, select **Immediate** or specify a time to transfer.
- Select the **Write Running to Startup Configuration** check box if it is a router..

Click **Next**

Result: The Work Order window appears.

Procedure 1-17 How to Restore an Old Configuration (Continued)**12** Click **Finish**.**Result:** An Information dialog box appears.**13** Click **OK** to dismiss the dialog box.**Result:** The Browse Job dialog box appears (Figure 1-45).**Figure 1-45** Browse Job Dialog Box**14** Click **Update Display**.**Result:** In the Run Status column, wait for the job to show **Succeeded**.

Transferring New Software to the LAN Switch

This section covers the transfer of files to the LAN switch (for example, to upgrade the software). This process is required a few times a year, typically when a new software image is sent by the manufacturer.

**IMPORTANT**

If you attempt to downgrade to a previous version, you may lose configuration information.

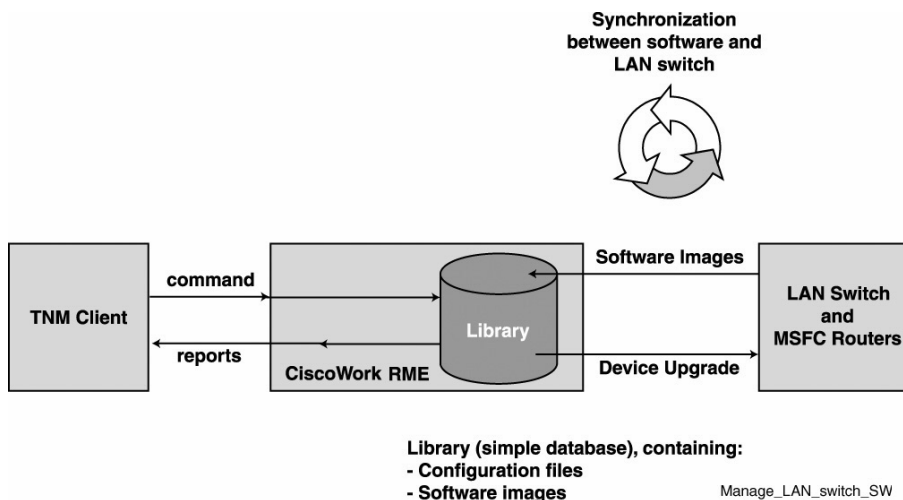
**IMPORTANT**

Motorola does not support scheduled upgrades. Do not use the Cisco scheduled upgrade.

**IMPORTANT**

You must contact Motorola System Support Center (SSC) before attempting this procedure as it may impact system performance.

Figure 1-46 shows the software management process for the LAN switch.

Figure 1-46 LAN Switch Software Management Process Diagram

Process 1-1 shows the process of transferring new software to the LAN switch.

Process 1-1 Transferring New Software to the LAN Switch

1	Copy the Catalyst image files (that is, the Catalyst Operating System (COS)) from a CD to the TNM client workstation. (See Procedure 1-18 on page 1-50 for information on how to copy the image files.)
2	Add the new images to the library. (The library is a simple database, provided by CiscoWorks2000, that holds configuration and image files and sorts them into different categories per device. Procedure 1-19 on page 1-51 describes how to add the new images to the library.)
3	Distribute the software image to the device. (Procedure 1-20 on page 1-53 describes how to distribute software images to the device.)
4	Verify that the new software version is loaded. (Procedure 1-21 on page 1-57 describes how to verify that the software image distribution is successful.)



NOTE

You must obtain the password for the UNIX user before performing this procedure.

Copying the Catalyst Image Files to the TNM Client and the Server

Procedure 1-18 describes how to copy Catalyst image files (the Catalyst Operating System (COS)) to the TNM client workstation. This procedure is used to upgrade the software version for the COS/Cisco Internet Operating System (IOS).

This is a process that involves copying the files from a CD to the TNM client workstation and then moving them to the Ethernet Switch Management Server (ESMS), where CiscoWorks2000 resides. The files are then moved to the library and then to the actual LAN switch.

Procedure 1-18 How to Copy the Catalyst Image Files to the TNM Client and the Server

1	On the TNM client, open a command prompt window.
2	On the TNM client, copy the Catalyst Supervisor/IOS image files under C:\temp. (If the directory does not exist, use mkdir c:\temp to create one first.)
3	Type c: and press Enter .
4	Type cd \temp and press Enter .
5	Type ftp 10.0.0.17 to access the ESMS for CiscoWorks2000. Result: The login prompt appears.
6	Type root for the UNIX user and type the password. Result: The root user is logged in.
7	Type cd /tmp and press Enter . Result: Display command successful appears.
8	Type bi and press Enter . Result: The display type is set to l .
9	Type put <name of your Catalyst Supervisor/IOS image file> . Result: The Display transfer is complete. This puts the files on the ESMS for CiscoWorks.
10	Upon successful transfer, type bye to exit.

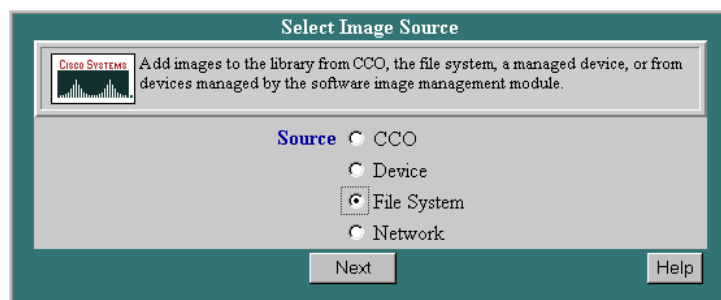
Adding New Images to the Library

Procedure 1-19 describes how add new images to the library.

Procedure 1-19 How to Add New Images to the Library

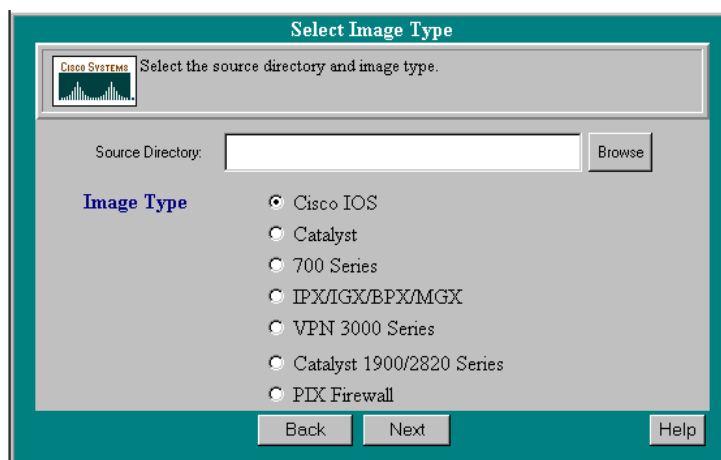
1	Open CiscoWorks2000.
2	Select Resource Manager Essentials in the navigation pane of the CiscoWorks2000 main window. Result: The Resource Manager Essentials suite appears.
3	Select Software Management , select Library , and then select Add Images . Result: The Select Image Source dialog box appears (Figure 1-47).

Figure 1-47 Select Image Source Dialog Box



4	Click the File System radio button, then click Next . Result: The Select Image Type dialog box appears (Figure 1-48).
----------	---

Figure 1-48 Select Image Type Dialog Box



5	In the Source Directory box, type /tmp .
----------	---

Procedure 1-19 How to Add New Images to the Library (Continued)

6	<p>Select Catalyst or Cisco IOS then click Next.</p> <p>Result: Software Management retrieves the files, analyzes them according to the selected image type, and then displays the Verify Image Type dialog box.</p>
7	<p>Verify that the Catalyst/IOS image Add to Library check box is selected.</p>
8	<p>Click Next.</p> <p>Result: A message reminds you that retrieving the necessary image attributes might take a while.</p>
9	<p>Click OK.</p> <p>Result: The Confirm Images dialog box displays the attributes for the software images.</p> <div data-bbox="485 697 584 808"> </div> <div data-bbox="669 728 781 768"> <p>NOTE</p> </div> <p>The amount of required disk space appearing at the bottom of the screen reflects only the selected images that were verified.</p>
10	<p>Click Next.</p> <p>Result: The images for which attributes could not be retrieved are displayed. If you are downloading images of several image types, such as boot loader, there is a separate editing screen for each.</p>
11	<p>Click Finish.</p> <p>Result: A message reminds you that the copy process might take a while.</p>
12	<p>Click OK to continue.</p> <p>Result: The images are added to the software library. After the process is complete, the Add to Library Summary displays the status of each image. The Status shows Successful.</p>
13	<p>To verify the success of the procedure, click Browse Library.</p> <p>Result: The new image is in the list.</p>

Distributing Software Images to the LAN Switch or MSFC Routers

Procedure 1-20 describes how to distribute Software Images to the LAN switch or MSFC routers.

Procedure 1-20 How to Distribute the Software Image to the LAN Switch or MSFC Routers

- 1 Select **Resource Manager Essentials** in the navigation pane of the CiscoWorks2000 main window.

Result: The Resource Manager Essentials suite appears.

- 2 Select **Software Management**, select **Distribution**, and then select **Distribute Images**.

Result: The Select Device Type dialog box appears (Figure 1-49).

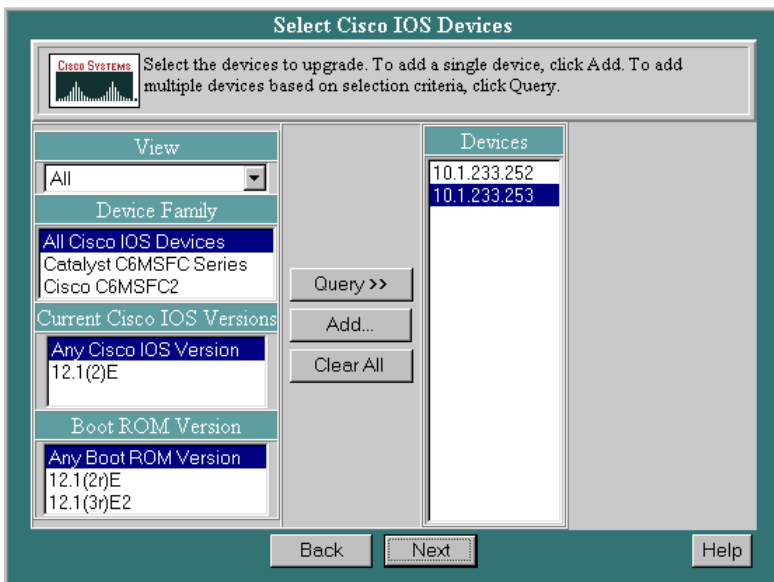
Figure 1-49 Select Device Type Dialog Box



- 3 Select **Catalyst** or **Cisco IOS**, then click **Next**.

Result: The Select Catalyst Devices or Select Cisco IOS Devices dialog box appears (Figure 1-50).

Figure 1-50 Select Catalyst Devices Dialog Box (Example)



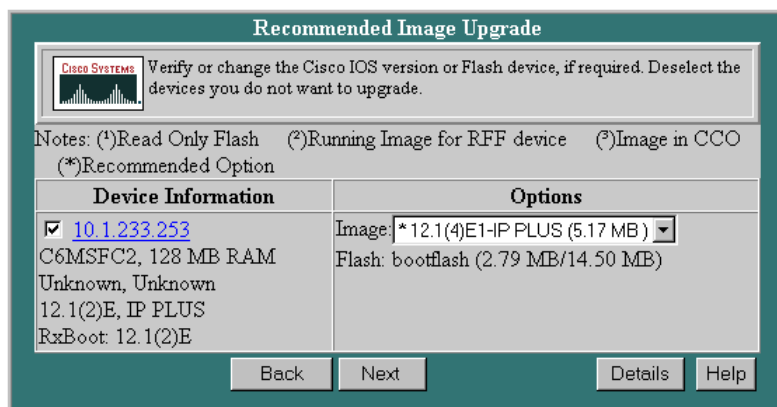
Procedure 1-20 How to Distribute the Software Image to the LAN Switch or MSFC Routers
(Continued)

4	IF you choose:	THEN:
	Catalyst Supervisor images	<ol style="list-style-type: none"> 1. In the View list, select All Catalysts. 2. In the Device Family list, select Catalyst 6000 Series. 3. Click Query. <p>Result: All Cisco Catalyst IP addresses appear in the Devices box.</p>
	Cisco IOS images	<ol style="list-style-type: none"> 1. In the View list, select All. 2. In the Device Family list, select All Cisco IOS Devices. 3. In the Current Cisco IOS Versions list, select Any Cisco IOS Version. 4. In the Boot ROM Version list, select Any Boot ROM Version. 5. Click Query. <p>Result: All Cisco MSFC router IP addresses appear in the Devices box.</p>

- 5 Hold the **Ctrl** key and click the left mouse button to select all the devices that you want to upgrade and click **Next**.

Result: The Recommended Image Upgrade dialog box appears (Figure 1-51).

Figure 1-51 Recommended Image Upgrade Dialog Box



Procedure 1-20 How to Distribute the Software Image to the LAN Switch or MSFC Routers
(Continued)

- 6
- Do the following:
1.

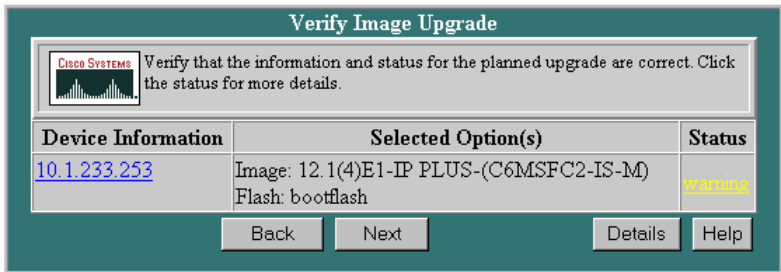
Select each check box for devices to upgrade or clear the check box for any devices you do not want to upgrade.
2.

For each device, select the image you want to upgrade to. If the Image list has an option for **bootflash**, you **must** select that option; do not select the slot option.
3.

Click **Next**.

Result: The Verify Image Upgrade dialog box appears (Figure 1-52).

Figure 1-52 Verify Image Upgrade Dialog Box



Procedure 1-20 How to Distribute the Software Image to the LAN Switch or MSFC Routers (Continued)

7

If a warning appears in the Status column, read the warning and then click **Next** if you want to continue.



IMPORTANT

If you are downgrading to an earlier version, you may lose some or all configuration.

Result: The screens that appear depend on the status of the devices you are downloading.

- If none of the devices pass the verification process, resolve the problem and resubmit the list of devices.
- If some devices do not pass, a message asks whether you wish to continue. Click **OK** to proceed or **Cancel** to return to the Verify Image Upgrade report.
- If more than one device passes the verification process, the Distribution Sequence dialog box appears.

To determine the upgrade order, select devices, one at a time, and click the **Move Up** and **Move Down** buttons. When the devices appear in the correct order, click **Next**.

Result: The Job Control Information dialog box appears (Figure 1-53).

Figure 1-53 Job Control Information Dialog Box

8

Type a brief message in **Job Description** field, including your name and image versions. Select **Immediately** or specify a time to upgrade.



CAUTION

The software upgrade uses a significant amount of bandwidth and causes service disruption. The LAN switch takes 5 minutes to reboot. Therefore, it is highly recommended that you do this when the system is not heavily loaded and only when instructed by Motorola service representatives.

Procedure 1-20 How to Distribute the Software Image to the LAN Switch or MSFC Routers
(Continued)

9	Select Reboot immediately after download . Do not select any of the check boxes under Select the job control options. Click Next . Result: The Work Order Report dialog box appears.
10	Double-check the message to ensure that it reflects your choices. Click Finish . Result: The Distribute Image Summary dialog box appears.
11	Depending on the status of your network, size of the image, and speed of your devices, the process will take anywhere from 5 to 30 minutes. Click Browse Job Status to view the status. Result: The Job Details dialog box appears.
12	Click Update until you see the job is completed. Result: The dialog box is updated.

Verifying the Software Image Distribution

Procedure 1-21 describes how to verify the software image distribution, which verifies if the software upgrade or re-installation was successful. You telnet to the switch to verify that the new software version is on the switch.

Procedure 1-21 How to Verify the Software Image Distribution

1	Type telnet <IP address of the LAN switch/router> and press Enter .
2	Type the <Telnet password> and press Enter .
3	Type show version and press Enter . Result: You should see your new version software loaded.

Checking Device Configuration Changes and CiscoWorks2000 Users Who Made Changes

This section describes how to check device configuration changes and determine who made them. This is useful when many people share job functions and need to coordinate adding features or updating the configuration. You can track changes made to the device configuration.

Checking Device Configuration Changes (Example 1)

Procedure 1-22 describes how to check the device configuration changes. This example shows **two versions of the same device** for a LAN switch.

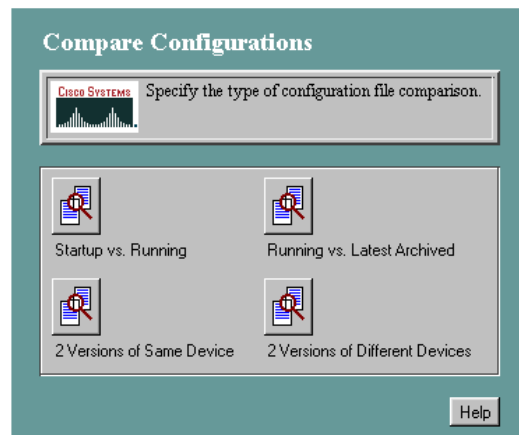
Procedure 1-22 How to Check Device Configuration Changes (Example 1)

- | | |
|----------|---|
| 1 | Select Resource Manager Essentials in the navigation pane of the CiscoWorks2000 main window.

Result: The Resource Manager Essentials suite appears. |
| 2 | Select Configuration Management and then select Compare Configurations .

Result: The Compare Configurations dialog box appears (Figure 1-54). |

Figure 1-54 Compare Configurations Dialog Box



Procedure 1-22 How to Check Device Configuration Changes (Example 1) (Continued)

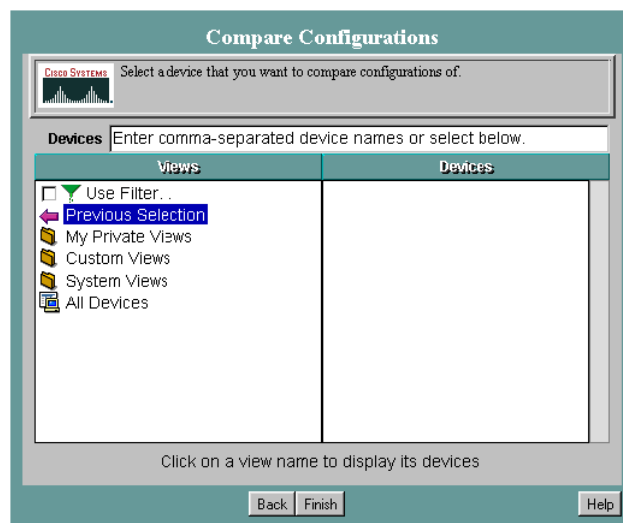
- 3** Click on one of the buttons. (This example shows **two versions of the same device.**)

**NOTE**

LAN switches only have a running version, so do not select **Startup vs Running** or **Running vs. Latest Archived** for a switch.

Result: The Compare Configurations dialog box appears (Figure 1-55).

Figure 1-55 Compare Configurations Dialog Box

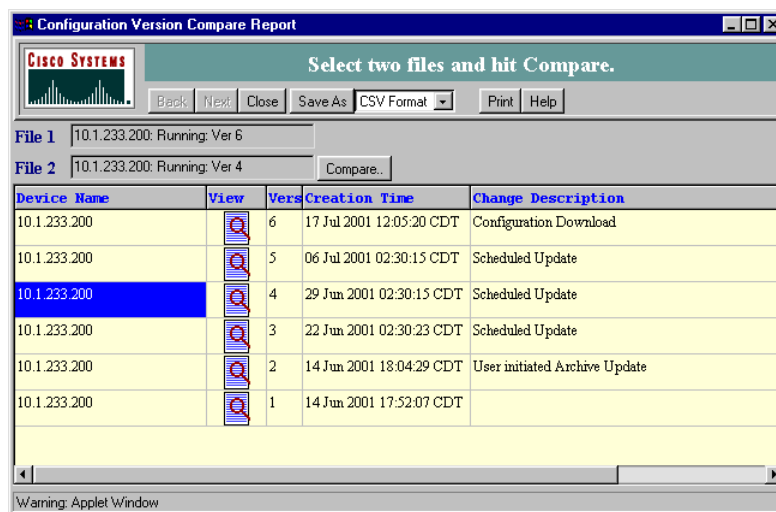


Procedure 1-22 How to Check Device Configuration Changes (Example 1) (Continued)

- 4** In the View area, select **All Devices** and then select the LAN switch in the Devices area. Click **Finish**.

Result: The Configuration Version Compare Report appears (Figure 1-56).

Figure 1-56 Configuration Version Compare Report



- 5** Click the first configuration file that you want to compare.

Result: The file name appears in the **File 1** field.

- 6** Click the second configuration file that you want to compare.

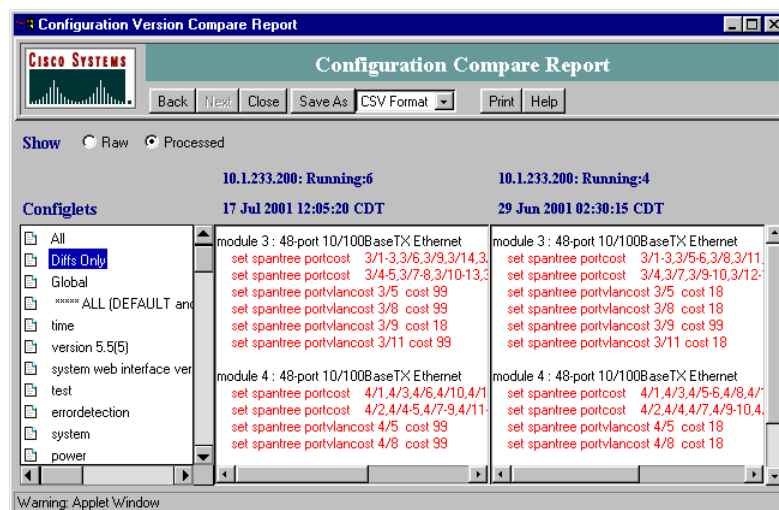
Result: The file name appears in the **File 2** field.

Procedure 1-22 How to Check Device Configuration Changes (Example 1) (Continued)

7 Click **Compare**.

Result: The Configuration Compare Report dialog box appears (Figure 1-57) showing **Diffs Only** (the differences between the two configurations are displayed in the panes).

Figure 1-57 Configuration Compare Report Dialog Box



8 Continue to Procedure 1-24 to find out who made the configuration changes.

Checking Device Configuration Changes (Example 2)

Procedure 1-23 describes how to check the device configuration changes. This example shows **Startup vs Running** for a router.

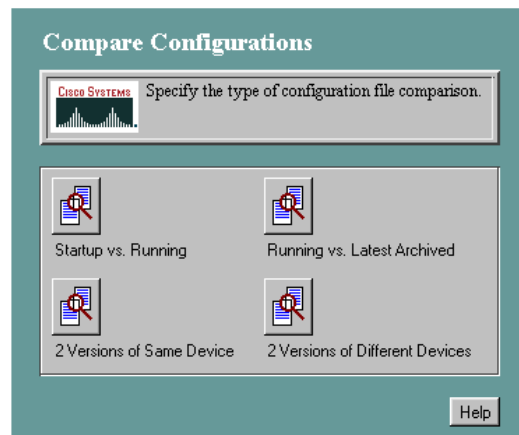
Procedure 1-23 How to Check Device Configuration Changes (Example 2)

- | | |
|----------|---|
| 1 | Select Resource Manager Essentials in the navigation pane of the CiscoWorks2000 main window.

Result: The Resource Manager Essentials suite appears. |
| 2 | Select Configuration Management and then select Compare Configurations .

Result: The Compare Configurations dialog box appears (Figure 1-58). |

Figure 1-58 Compare Configurations Dialog Box

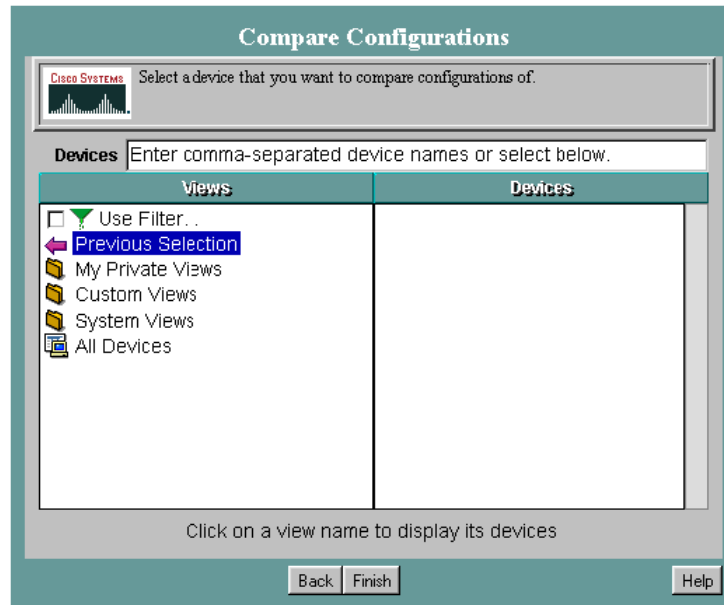


Procedure 1-23 How to Check Device Configuration Changes (Example 2) (Continued)

3 Click one of the buttons. This example shows **Startup vs Running** for a router.

Result: The Compare Configurations dialog box appears (Figure 1-59).

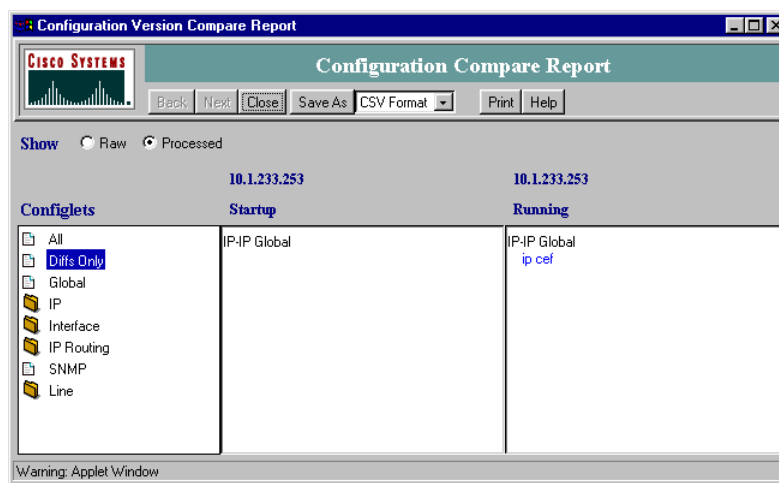
Figure 1-59 Compare Configurations Dialog Box



4 In the View area, select **All Devices** and then select the router in the Devices area. Click **Finish**.

Result: The Configuration Version Compare Report appears displaying the **Diffs Only** folder in the Configlets pane (Figure 1-60). The differences between the two configurations are displayed in the Startup and Running panes.

Figure 1-60 Configuration Version Compare Report



5 Continue to Procedure 1-24 to find out who made the configuration changes.

Verifying CiscoWorks2000 Users Who Made Configuration Changes

Once you have verified that the configurations are different, Procedure 1-24 describes how to check to see who made the change, so that you can contact the person and find out why it was made.



NOTE

The change must have occurred within the last 24 hours.

Procedure 1-24 How to Verify the CiscoWorks2000 Users Who Made the Configuration Changes

- 1 Select Resource Manager Essentials, select **24-Hour Reports**, and then select **Change Audit Report**.

Result: The Change Audit 24-Hour Report appears (Figure 1-61).

Figure 1-61 Change Audit 24-Hour Report

Device Name	User Name	Application Name	Host Name	Creation Time	Connection Mode	Category	Message	View Details	Grouped Records
10.1.233.200	admin	Config Editor	N/A	17 Jul 2001 12:05:30 CDT	N/A	Config	Configuration Download	Details	More Records

End of Records



NOTE

(If you are unsure when the change occurred, select Resource Manager Essentials, select **Change Audit**, and then select **Search Change Audit**.)

- 2 Identify the user who made the changes to the device by using the User Name column.

Displaying LAN Switch Alarms in HP OpenView

The following section describes how you can also display alarm information and traps for the LAN switch using HP OpenView. HP OpenView provides the following alarm display information:

- **Cisco Alarm category** — appears in the Alarm Categories dialog box, used to access an Alarm Browser window where you can view Cisco-generated traps.



NOTE

A CiscoWorks Alarm categories also appears in the Alarm Categories dialog box, but it is not activated for this release.

- **Default traps** — provides Cisco trap definitions that are integrated with HP OpenView. The Cisco Device traps provide alarm information for the Ethernet LAN switch and MSFC routers.
- **Internet submap** — shows the LAN switch and the routers for each zone. Labels on the icons vary according to your system (for example; z001lans01, z001msfc01, z12lans01, z120msfc01). The Internet map shows a Layer 3 subnet and does not show Layer 2 connectivity. This means that it does not show the physical connectivity between the devices in the zone core to the LAN switch.



NOTE

See Volume 2, *Fault Management* and **FullVision INM Online Help** for more information about displaying alarms and viewing the Cisco Device Traps.

Managing the WAN Switch

The WAN switch is managed by the network management tools provided by Preside® Multiservice Data Manager (MDM) from Nortel® Networks. Preside MDM is installed on the WAN Switch Management Server (WSMS).

Preside MDM allows you to view inventory for the WAN switch and view alarms. You can also use the MDMWeb online browser to view alarms and perform some of the same tasks as the Preside MDM application. This chapter contains the following topics:

- "Managing Security Access" on page 2-2
- "System Diagram" on page 2-4
- "Accessing Preside MDM" on page 2-4
- "Performing Inventory on the WAN Switch" on page 2-9
- "Backing Up and Restoring the WAN Switch" on page 2-11
- "Downloading Software to the WAN Switch" on page 2-18
- "Adding a WAN Switch" on page 2-23
- "Connecting to the WAN Switch by Command Line" on page 2-29
- "Collecting and Displaying Performance Information" on page 2-34
- "Viewing the Status of WAN Switch Components" on page 2-38
- "Displaying WAN Switch Alarms" on page 2-42
- "Using Preside MDM for Fault Management" on page 2-44
- "Using Preside MDM for Fault Management" on page 2-44
- "Using the MDMWeb" on page 2-47



CAUTION

Do not tamper with factory configuration settings for the network transport device. This includes software configuration, firmware release, password, and physical connections. Motorola® has configured and connected this device to meet very specific performance requirements. Tampering with this device may result in unpredictable system performance or catastrophic failure. In the event you need to make configuration changes you must contact Motorola System Support Center (SSC) before attempting any configuration changes or software upgrades of network transport devices.

Managing Security Access

Preside MDM provides the following accounts:

- **mdmusr** (user) account: account recommended for general use of Preside MDM (such as viewing reports and monitoring performance).
- **mdmmgr** (manager) account: allows certain managerial tasks to be performed that are not allowed for **mdmusr**. For example, **mdmmgr** can also use Preside to configure the WAN switch.



NOTE

The passwords are confidential and provided by Motorola to approved users. Contact your Motorola support person for more information.

Table 2-1 describes the account types for client access along with the options that account can use and the related procedure in this booklet.



NOTE

For menu options that are not shown, refer to the Preside online help for a description.

Table 2-1 Account Types for Client Access

Account	Options for Client Access	Procedure
mdmusr	Network Viewer	"Viewing the Status of WAN Switch Components" on page 2-38
	Alarm Display (active and log mode)	"Displaying WAN Switch Alarms" on page 2-42
	Component Information Viewer	"Accessing Component Information Viewer" on page 2-41
	Performance Viewer	"Collecting and Displaying Performance Information" on page 2-34
	Command Console	"Connecting to the WAN Switch by Command Line" on page 2-29
	Inventory Reports	"Performing Inventory on the WAN Switch" on page 2-9

Table 2-1 Account Types for Client Access (Continued)

Account	Options for Client Access	Procedure
mdmmgr	All options listed above for mdmusr , plus additional options that are limited to mdmmgr, as follows:	
	Service Data Backup	"Manually Backing Up the WAN Switch" on page 2-14
	Service Data Restore	"Restoring the WAN Switch" on page 2-16
	Software Download and Configuration	"Downloading Software to the WAN Switch" on page 2-18

Table 2-2 describes the account types for web access and the related procedures.

Table 2-2 Account Types for Web Access

Accounts	Options for Web Access	Procedure
mdmusr and mdmmgr	Alarm Display	"Displaying Alarms Using MDMWeb" on page 2-55
	Command Console	"Connecting to the WAN Switch Using Command Line Via MDMWeb" on page 2-53
	Component Information Viewer	Receives information from the Preside server, so the information is the same as the client access. See "Accessing Component Information Viewer" on page 2-41 for more information.

Table 2-3 describes the two user accounts created at the WAN switch itself, through Telnet Command Line Interface (CLI) session.

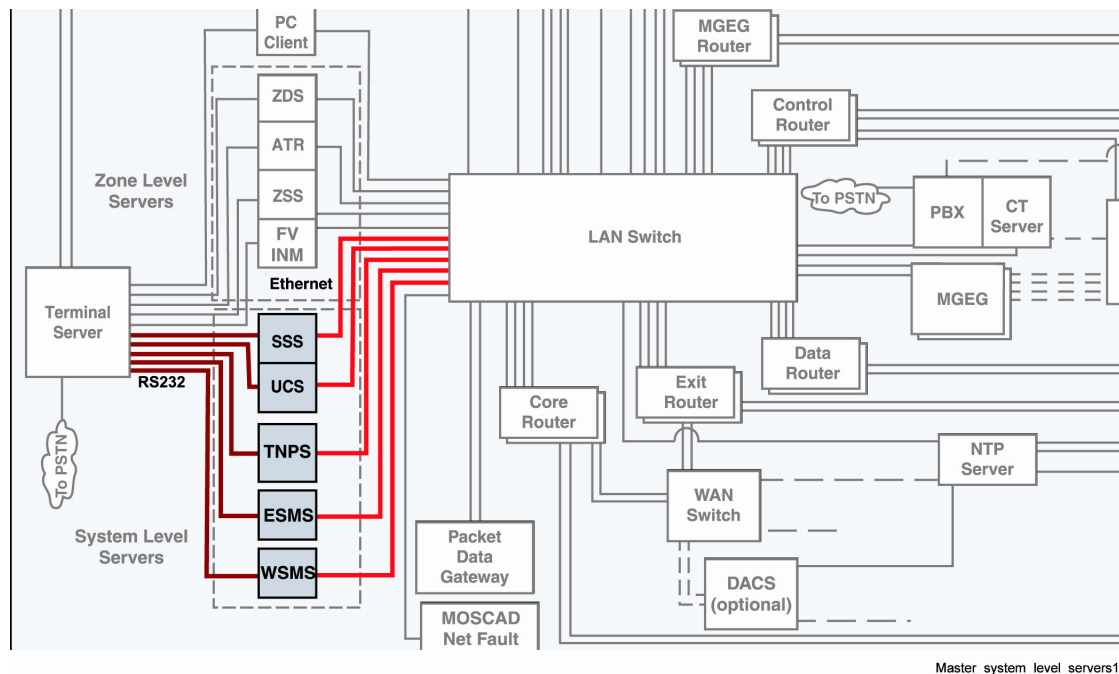
Table 2-3 Account Types for WAN Switch

Type of Account	Access
mdmusr	Read-only access to the WAN switch to list and display the switch components and their status.
mdmmgr	Read and write access rights to the WAN switch.

System Diagram

Figure 2-1 shows how the WSMS, where Preside MDM resides, fits into the system master site.

Figure 2-1 System Diagram Example



Accessing Preside MDM

You can access Preside MDM functions in the following ways:

- Windows® 2000 client workstation (initial launch and relaunch). (You can use the Network Management Client or the Transport Network Management Client.)

- MDMWeb (see "Using the MDMWeb" on page 2-47)



NOTE

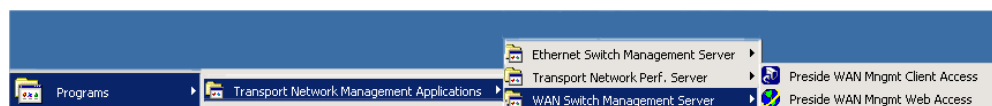
The Windows 2000 client workstation must be able to ping the Preside MDM server. From a command prompt window on the Windows 2000 client workstation, verify ping by typing **ping 10.0.0.16** and wait for the ping reply.

Access Points for Preside MDM

On the Windows 2000 client workstation, you can access Preside MDM from two places:

- From the Start menu, select **Programs**, select **Transport Network Management Applications**, select **WAN Switch Management Server**, and then select **Preside WAN Mngmt Client Access** (Figure 2-2).

Figure 2-2 Transport Network Management Applications Menu



- From the desktop, double-click the **Preside Client Access** icon (Figure 2-3).

Figure 2-3 Preside Client Access Desktop Icon



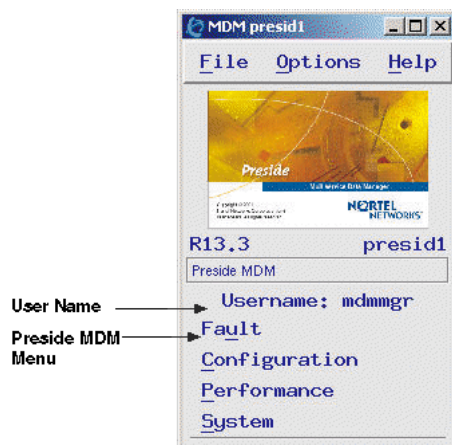
Launching Preside MDM - Client Workstation


Procedure 2-1 describes how to launch Preside MDM.

Procedure 2-1 How to Launch Preside MDM

1	<p>From the desktop, double-click the Preside Client Access icon.</p> <p>Result: The Common Desktop Environment (CDE) login page from the application server appears.</p>
2	<p>In the Username field, type mdmusr or mdmmgr (as applicable) and press Enter.</p>
3	<p>In the Password field, type the password and press Enter.</p> <p>Result: The Preside MDM main window appears (Figure 2-4).</p>

Figure 2-4 Preside MDM Main Window



4	<p>Navigate through the Preside MDM application using the menu options. Each window has access to drop-down menu options from the Menu bar. (See Table 2-4 for a detailed listing.)</p> <div data-bbox="391 1409 748 1514">  <div data-bbox="513 1430 748 1482">NOTE</div> </div> <p>The menu options that are available depend on your user rights.</p>
---	---

Menu Options

Table 2-4 contains the menu options for the Preside users. Menu options marked with an asterisk (*) are covered in this booklet. For procedures related to the unmarked menu options or for descriptions of the menu options, see the **Preside Online Help**.

Table 2-4 Menu Options for Preside MDM

Main Window Menu Options	Submenu Options for mdmmgr	Submenu Options for mdmusr
Fault	Network Viewer* Alarm Display: Active* Alarm Display: Log* Alarm Help Network Status bar Component Information Viewer* Component Status Display	Network Viewer* Alarm Display: Active* Alarm Display: Log* Alarm Help Network Status bar Component Information Viewer* Component Status Display
Configuration	Passport Devices —Component Provisioning —Administration <ul style="list-style-type: none"> • Service Data Backup (Legacy)* • Service Data Restore (Legacy)* • Software Download and Configuration* • Network Activation Tool —Inventory Reports*	Passport Devices <ul style="list-style-type: none"> • Inventory Reports*
Performance	Passport/DPN Performance Viewer*	Passport/DPN Performance Viewer*
System	Utilities <ul style="list-style-type: none"> • Unix Access • Remote Access • Command Console* • Online Documentation • Memory Utilization • Network Model Shared Memory Utilization 	Utilities <ul style="list-style-type: none"> • Unix Access • Remote Access • Command Console* • Online Documentation • Memory Utilization • Network Model Shared Memory Utilization

Relaunching Preside MDM - Client Workstation

Procedure 2-2 describes how to relaunch Preside MDM in the UNIX® environment if you exited the automatically launching window.

Procedure 2-2 How to Relaunch Preside MDM

1	Do one of the following to access the root # prompt:	
	IF	THEN
	An Xterm Console window is already open	Click the Console Xterm window and press Enter . Result: The root # prompt appears.
	An Xterm Console window is not open	<ol style="list-style-type: none"> 1. Right-click on the desktop to open the Workspace menu. 2. Select Programs and then select Console to open a Console window. Result: An Xterm console window appears.
2	Type nmstool & and press Enter . Result: The Preside MDM application appears. See Figure 2-4, "Preside MDM Main Window" on page 2-6.	

Exiting Preside MDM

Procedure 2-3 describes how to exit Preside MDM in the UNIX environment.

Procedure 2-3 How to Exit Preside MDM

1	On the Solaris® Sun® task bar, click Exit . Result: The Logout Confirmation appears.
2	Click OK and then click Yes to exit. Result: Preside MDM and the UNIX environment close.

Obtaining the WAN Switch Name

Many procedures in this document require you to know the WAN switch name. Please obtain the WAN switch name from the Passport switch engineer.

Performing Inventory on the WAN Switch

The Passport Inventory Reports tool lets you produce reports for the modules in a Passport group or for a specific module.

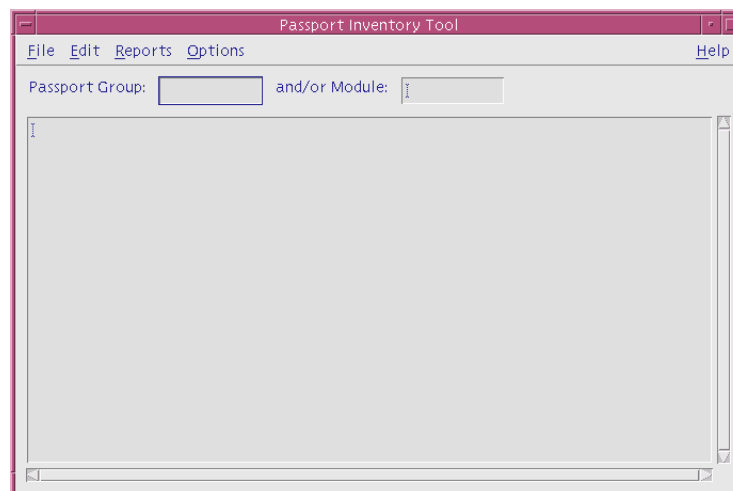
Procedure 2-4 describes how to perform inventory on the WAN switch.

Procedure 2-4 How to Perform Inventory on the WAN Switch

- 1 From the Preside MDM main window, click **Configuration**, select **Passport Devices**, and then select **Inventory Reports**.

Result: The Passport Inventory Tool window appears (Figure 2-5).

Figure 2-5 Passport Inventory Tool Window



- 2 In the Passport Group box, type **GST**. In the and/or Module box, type **<WAN switch name>**.

Procedure 2-4 How to Perform Inventory on the WAN Switch (Continued)

3 From the Reports menu, select **Software Report**.

Result: The Passport Authentication dialog box appears (Figure 2-6).

**NOTE**

This dialog box does not appear for subsequent logins.

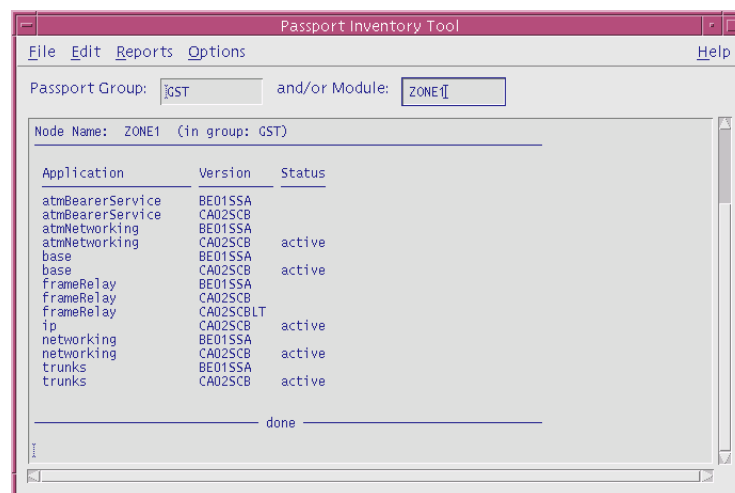
Figure 2-6 Passport Authentication Dialog Box



4 In the User ID field, type **mdmusr** or **mdmmgr** (as applicable), enter the password, and press **Enter**.

Result: The Passport Inventory Tool window appears, which shows the software report on the <WAN Switch name>. (In Figure 2-7, “zone1” is the switch name; your switch name will be different.)

Figure 2-7 Passport Inventory Tool Window



5 From the Reports menu, select **Card Inventory**.

Result: The Card Inventory Options window appears.

Procedure 2-4 How to Perform Inventory on the WAN Switch (Continued)

6 Click **OK**.

Result: The Passport Inventory Tool window shows the Passport Card Inventory report for the entered WAN switch (Figure 2-8).

Figure 2-8 Card Inventory Report Window

Node	Card	Type	Inserted	Serial #	Product Code	LP
ZONE1	0	CP	CP	NNTM03505TNU	NTNQ01AA-04	Lp/0
ZONE1	1	HSSI	HSSI	NNTM03504MAG	NTNQ27AA-03	Lp/1
ZONE1	2	HSSI	HSSI	NNTM03506CTM	NTNQ27AA-03	Lp/2
ZONE1	3	none	32pDS1Msa	NNTM03503WKN	NTNQ27AA-07	None
ZONE1	4	none	none	None	None	None
ZONE1	5	HSSI	HSSI	NNTM035039XE	NTNQ27AA-03	Lp/5
ZONE1	6	HSSI	HSSI	NNTM03506G43	NTNQ27AA-03	Lp/6
ZONE1	7	none	none	None	None	None
ZONE1	8	none	none	None	None	None
ZONE1	9	none	none	None	None	None
ZONE1	10	8pDS1	8pDS1	NNTM03505NPX	NTNQ16AA-02	Lp/10
ZONE1	11	none	none	None	None	None
ZONE1	12	V11	V11	NNTM0350538U	NTNQ12AA-02	Lp/12
ZONE1	13	none	none	None	None	None
ZONE1	14	8pDS1Atm	8pDS1Atm	NNTM03504WWQ	NTNQ49AA-03	Lp/14
ZONE1	15	none	none	None	None	None

7 From the File menu, select **Exit** to close the window.

Backing Up and Restoring the WAN Switch

Table 2-5 lists the types and frequencies of WAN switch configuration file backups and restores.

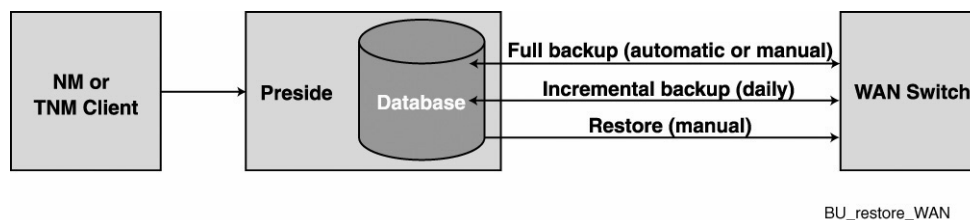
Table 2-5 Recommended Frequency of Backup and Restores

Type of Backup/Restore	When performed
Full backup	A one-time full WAN switch backup for all configuration files (service data) from the WAN switch to the WSMS is performed immediately after Preside MDM is installed. This backup is performed automatically and is set up by Motorola. See Volume 9, <i>Network Transport Applications Installation and Configuration</i> .

Table 2-5 Recommended Frequency of Backup and Restores (Continued)

Type of Backup/Restore	When performed
Incremental backup	This process only backs up configuration changes or additions on the WAN switch since the last backup. Preside MDM and the UNIX crontab setup utility on the WSMS server are configured and used to schedule an incremental backup automatically at 12 AM, Monday through Saturday. This backup is performed automatically and is set up by Motorola. See Volume 9, <i>Network Transport Applications Installation and Configuration</i> .
Manual full backup	A periodic backup can be performed as needed in using Preside's Passport Service Data Backup. You can use the Passport Service Data Restore option to restore a configuration. See Procedure 2-7, "How to Restore the WAN Switch," on page 2-15 .
Selective restore	As needed if there is a problem with new software, and you want to revert to a previous configuration. Preside MDM also allows you to selectively restore the WAN switch configuration files. See Procedure 2-7, "How to Restore the WAN Switch," on page 2-15.

Figure 2-9 shows the backup and restore process for the WAN switch configuration files.

Figure 2-9 Preside Backup and Restore Process**NOTE**

Since Preside MDM does not provide a mechanism to remove or override old backup files, manual full backups should not be performed more than necessary in order to avoid filling up the WSMS hard drive. Usually, a full backup followed by an incremental backup provides sufficient resource storage.

Obtaining the Provisioning Mode

Obtaining the provisioning mode is necessary to perform several procedures. However, since the WAN switches only allow one user at a time to be in the provisioning mode, you may initially be unable to obtain the provisioning mode (such as when another user with administrator level privileges has logged in to use the application and did not log out).

Procedure 2-5 describes how to obtain the provisioning mode when a conflict exists using a force command that disconnects an idle login and obtains the provisioning mode.

Procedure 2-5 How to Obtain the Provisioning Mode

1	<p>Telnet to <the IP address of the WAN Switch>, log on as mdmmgr and enter the <WAN switch mdmmgr password>.</p> <div data-bbox="334 705 431 814"> </div> <div data-bbox="456 730 691 781"> <p>NOTE</p> </div> <p>You must obtain password information from the Passport switch engineer.</p>				
2	<p>At the <passport prompt>, type st pr and press Enter.</p>				
3	<p>Select one of the following:</p> <table border="1"> <thead> <tr> <th data-bbox="329 961 787 1003">IF the following lines appear:</th><th data-bbox="795 961 1534 1003">THEN...</th></tr> </thead> <tbody> <tr> <td data-bbox="329 1014 787 1144"> Prov <messages> ok <time> </td><td data-bbox="795 1014 1534 1144"> At the <passport prompt>, type end pr and press Enter. Result: The following appears: Prov ok <time> </td></tr> </tbody> </table>	IF the following lines appear:	THEN...	Prov <messages> ok <time>	At the <passport prompt>, type end pr and press Enter . Result: The following appears: Prov ok <time>
IF the following lines appear:	THEN...				
Prov <messages> ok <time>	At the <passport prompt>, type end pr and press Enter . Result: The following appears: Prov ok <time>				
	<table border="1"> <tbody> <tr> <td data-bbox="329 1167 787 1329"> Prov Session <session information> is in provisioning mode. command failed <time> </td><td data-bbox="795 1167 1534 1434"> <ol style="list-style-type: none"> At the <passport prompt>, type st -force pr and press Enter. Result: The last line of display appears: ok <time> Type PROV 3> end pr and press Enter. Result: The following lines appear: Prov ok <time> </td></tr> </tbody> </table>	Prov Session <session information> is in provisioning mode. command failed <time>	<ol style="list-style-type: none"> At the <passport prompt>, type st -force pr and press Enter. Result: The last line of display appears: ok <time> Type PROV 3> end pr and press Enter. Result: The following lines appear: Prov ok <time> 		
Prov Session <session information> is in provisioning mode. command failed <time>	<ol style="list-style-type: none"> At the <passport prompt>, type st -force pr and press Enter. Result: The last line of display appears: ok <time> Type PROV 3> end pr and press Enter. Result: The following lines appear: Prov ok <time> 				

Manually Backing Up the WAN Switch

Procedure 2-6 describes how to manually back up data from the WAN switch to the Preside server.

Procedure 2-6 How to Manually Back Up the WAN Switch

1



NOTE

Before performing this procedure, ensure that no one holds the provisioning mode. See Procedure 2-5.

2

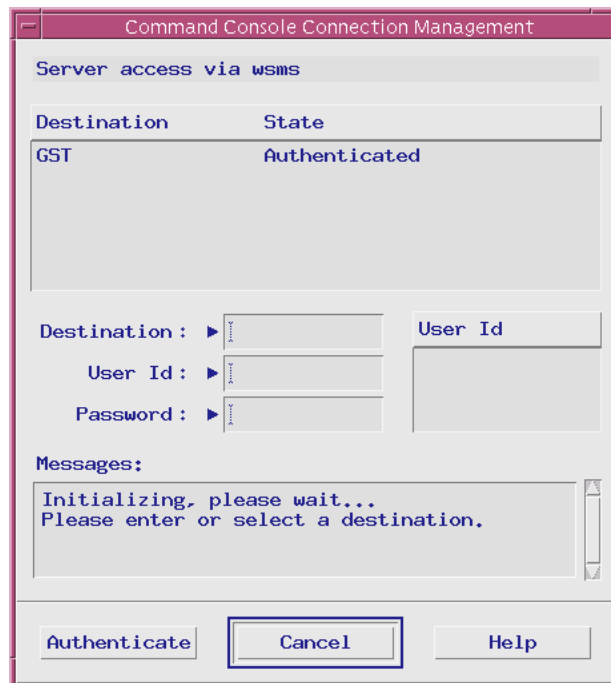
Launch Preside (see "Accessing Preside MDM" on page 2-4) and log on as **mdmmgr**.

3

From the Preside MDM main window, click **Configuration**, select **Passport Devices**, select **Administration**, and select **Service Data Backup (Legacy)**.

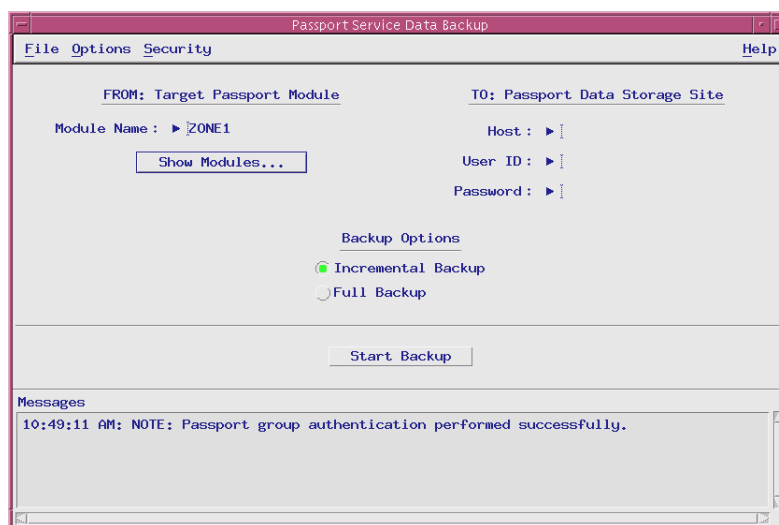
Result: The Command Console Connection Management dialog box (Figure 2-10) and the Passport Service Data Backup window (Figure 2-11) appear.

Figure 2-10 Command Console Connection Management Dialog Box



Procedure 2-6 How to Manually Back Up the WAN Switch (Continued)

- 4** From the Command Console Connection Management dialog box, do the following to connect to the WAN switch:
1. Select **GST**.
 2. Type **mdmmgr** for the user ID and then type the password.
 3. Click **Authenticate**.
- Result:** The dialog box closes.
- 5** From the Passport Service Data Backup window, click **Show Modules**.
- Result:** The Modules List window appears.
- 6** Select one of **<WAN Switch name>** that you want to back up and click **OK**.
- Result:** **<WAN Switch name>** appears on the Module Name field. (In the example in Figure 2-11, “ZONE1” is the switch name; your switch name will be different.)

Figure 2-11 Passport Service Data Backup Window

- 7** Type your Preside Server IP address at the Host field and your login name and password. For example:
- Host: **10.0.0.16**
 - User ID: **mdmmgr**
 - Password: **<mdmmgr password>**

Procedure 2-6 How to Manually Back Up the WAN Switch (Continued)

8	<p>Select Full Backup and click Start Backup.</p> <p>Result: The Service Data Backup in Progress window appears. Once the backup is complete, the message window closes automatically and Backup successfully appears in the Messages area. This procedure backs up to /export/home/mdmmgr.</p> <div data-bbox="391 436 456 541"> </div> <div data-bbox="514 464 748 512"> NOTE </div> <p>If the backup fails or an error occurs, ensure that no other user holds the provisioning mode. Provisioning mode becomes a problem if another user with administrator level privileges has logged in to use the application and did not log out. You must contact that user and have them log out.</p>
9	<p>From the File menu, select Exit to close the window.</p>

Restoring the WAN Switch

Procedure 2-7 describes how to restore data to the WAN switch. You should only restore the WAN switch if there is a problem with new software, and you want to revert to a previous configuration.


IMPORTANT

You must contact Motorola System Support Center (SSC) before attempting this procedure as it may impact system performance.

Procedure 2-7 How to Restore the WAN Switch

1	<div data-bbox="391 1297 456 1402"> </div> <div data-bbox="514 1325 748 1373"> NOTE </div> <p>Before performing this procedure, ensure that no one holds the provisioning mode. See Procedure 2-5.</p>
2	<p>Launch Preside (see "Accessing Preside MDM" on page 2-4) and log on as mdmmgr.</p>
3	<p>From the Preside MDM main window, click Configuration, select Passport Devices, Administration, and then Service Data Restore (Legacy).</p> <p>Result: The Command Console Connection Management dialog box (Figure 2-10) and the Passport Service Data Restore window (Figure 2-12) appear.</p>

Procedure 2-7 How to Restore the WAN Switch (Continued)

- 4** From the Command Console Connection Management dialog box, do the following to connect to the WAN switch:
1. Select **GST**.
 2. Type **mdmmgr** for the user ID and enter the password.
 3. Click **Authenticate**.
- Result:** The dialog box closes.

- 5** In the FROM: Passport Data Storage Site form of the Passport Service Data Restore window (Figure 2-12) enter the required information as follows:
- Source Module: <**WAN Switch name**> from which you would like to restore data
 - Host: **10.0.0.16**
 - User ID: **mdmmgr**
 - Password: <**mdmmgr password**>

Figure 2-12 Passport Service Data Restore Window

- 6** Click **Show Modules**.
- Result:** The MdlDialogShell dialog box appears.
- 7** Select a Passport backup in the Modules in group list and click **OK**.
- Result:** The Target Module text box shows the selected <**WAN switch name**>.

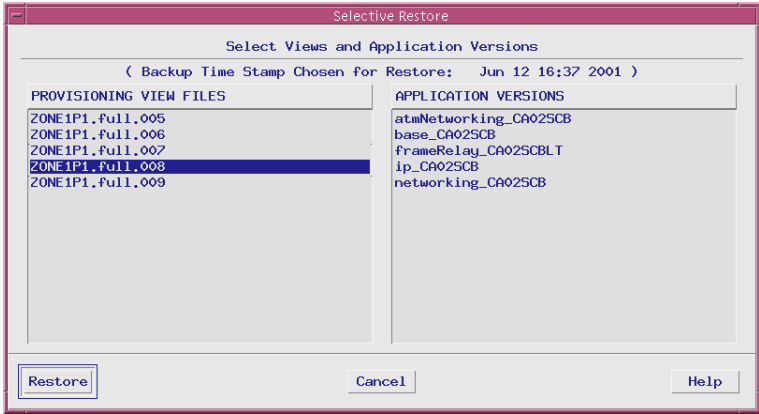
Procedure 2-7 How to Restore the WAN Switch (Continued)

8

Click **Selective Restore**.


Result: The Passport Service Data Restore window appears, followed by the Selective Restore dialog box (Figure 2-13).

Figure 2-13 Selective Restore Dialog Box



9

On the left side of the Selective Restore dialog box, choose a configuration file to restore (for example, <WAN Switch name>.full.008).



NOTE

You cannot restore a current view file that has been modified but not saved yet. Do not perform this procedure unless you know which file to restore.

10

Click **Restore**.

Result: The Passport Service Data Restore window appears. The Messages area of the Passport Service Data Restore window shows the following message:
The target module <WAN Switch name> has been re-stored successfully.
Passport Service Data Restore process exiting.

11

From the File menu, select **Exit** to close the window.

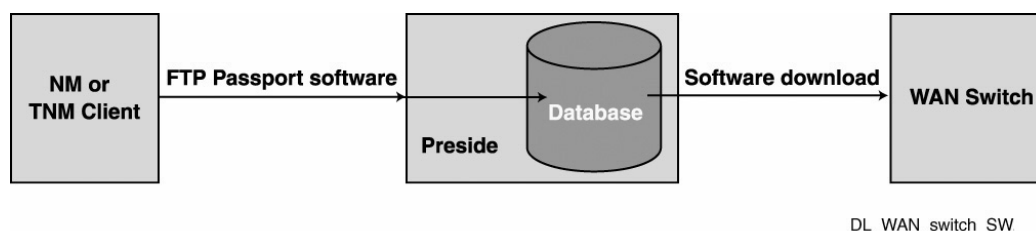
Downloading Software to the WAN Switch



The Software Distribution tool on Preside MDM allows you to download software from the Preside MDM server to managed WAN switches.

Figure 2-14 shows the software management process, using Preside MDM.

Figure 2-14 Preside Software Management Process



NOTE

Before performing this procedure, you must meet the following requirements:

- Have the proper knowledge and experience to perform this procedure. For example, you must be experienced with using FTP.
- Obtain the new software CD. You may need to find the FTP location.
- Identify the file name(s) for the software (software could be one file or several files).

Obtaining the New Software

Procedure 2-8 describes how to obtain the new software. This procedure assumes that the new software was transferred (using ftp) to the WSMS server where Preside MDM resides. The following is an example procedure; your file names could vary.



NOTE

You must contact Motorola System Support Center (SSC) before attempting this procedure.

Procedure 2-8 How to Download Software to the WAN Switch

1	Log on to the Preside MDM as mdmmgr . Result: The Preside MDM application launches automatically with the properly assigned user rights. (Figure 2-4 shows the Preside MDM main window.)
2	From the Start menu, select Programs , select Accessories , and then select Command Prompt . In the Command prompt window, type ftp 10.0.0.16 to access the WSMS for Preside MDM. Result: The login prompt appears.
3	Type mdmmgr for the UNIX user and type the password. Result: The mdmmgr user is logged in.
4	Type pwd and press Enter . Result: The directory is /export/home/mdmmgr/. If the new software is a tar'ed file from Nortel, you must FTP the file to be under /export/home/mdmmgr/.
5	Type bi and press Enter . Result: The display type is set to l .
6	Type put <name of your passport software> . Result: The Display transfer is complete. This puts the files on the WSMS.
7	Upon successful transfer, type bye to exit.
8	To untar the file, type tar -xvf <name of file>.tar and press Enter . (If you do not know the software version, contact Nortel Technology.)
9	Continue to Procedure 2-9.

Downloading the Software

Procedure 2-9 describes how to perform the software download.

**NOTE**

You must contact Motorola System Support Center (SSC) before attempting this procedure.

Procedure 2-9 How to Download Software

- 1 Click on the Preside MDM main window. Select **Configuration** and select **Passport Devices**. Select **Administration** and then select **Software Download and Configuration**.

Result: The Command Console Connection Management (Figure 2-15) dialog box and the Passport Software Distribution & Configuration window (Figure 2-16) appear.

Figure 2-15 Command Console Connection Management Dialog Box

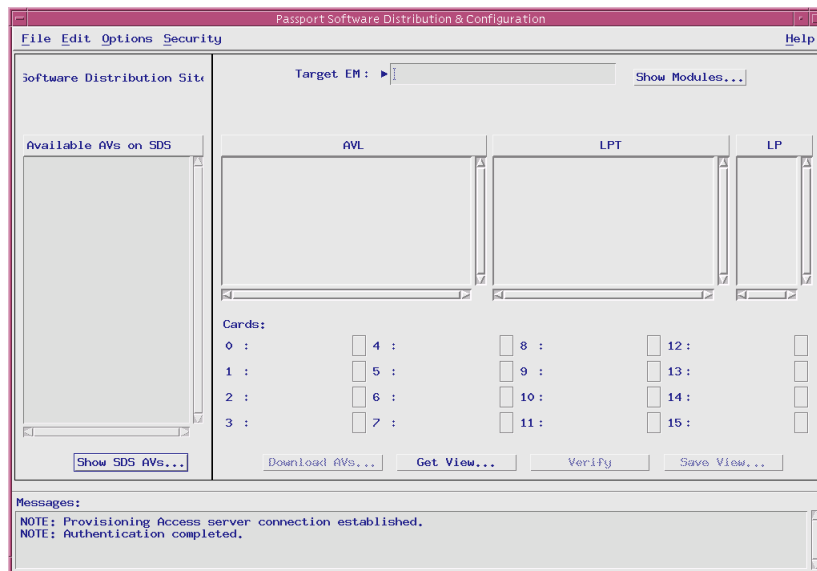
- 2 From the Command Console Connection Management dialog box do the following:
 1. Select **GST**.
 2. Type **mdmmgr** for the user ID and enter the password.
 3. Click **Authenticate**.

Result: The dialog box closes.

Procedure 2-9 How to Download Software (Continued)

- 3 From the Passport Software Distribution & Configuration window, click **Show Modules** (Figure 2-16).

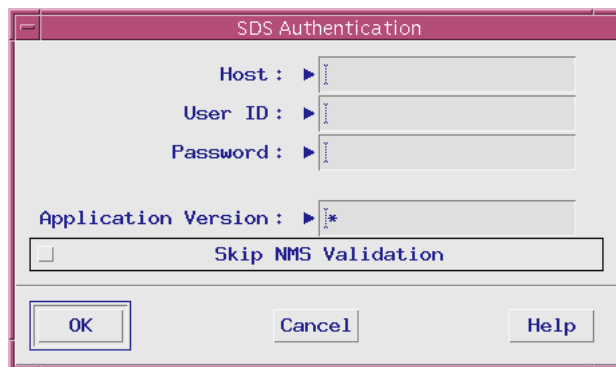
Figure 2-16 Passport Software Distribution & Configuration Window




- 4 Select the target <WAN Switch name> and click **OK**.
- 5 Click **Show SDS AVs** on the lower left side of the Software Distribution Window. (AVs means “Available List”.)

Result: The SDS Authentication dialog box appears (Figure 2-17).

Figure 2-17 SDS Authentication Dialog Box



Procedure 2-9 How to Download Software (Continued)

6	<p>Enter the following:</p> <ul style="list-style-type: none"> • Host: 10.0.0.16 • User ID: mdmmgr • Password: <mdmmgr password> <p>Click OK.</p> <p>Result: All available software on SDS appears.</p>
7	<p>Select the software from the list that you would like to download to the desired WAN switch (for example, “frameRelay_CD01C”).</p> <div data-bbox="488 638 586 747">  </div> <div data-bbox="610 663 846 716"> <p>NOTE</p> </div> <p>The software version “CD01C” in the above example is variable. Your software version may be this version or higher.</p>
8	<p>Click Download AVs.</p> <p>Result: The Downloading AVs window appears, followed by the Processor Targets window.</p>
9	<p>Select i960 and ppc, and then select OK.</p> <p>Result: The Downloading notice window appears. Wait until completed. (The amount of time depends on the size of file and the bandwidth of the link.) The Downloading notice window closes automatically. The Messages area of the Software Distribution & Configuration window shows the Operation completed message.</p>
10	<p>In the Messages area, scroll up and make sure that all operations completed successfully.</p>
11	<p>From the File menu, select Exit to close the window.</p>

Adding a WAN Switch

This section contains various procedures to log on to Preside MDM as administrator, select the network type, add the WAN switch, and then verify the success of the process.

Logging On as Administrator

Procedure 2-10 describes how to log on as administrator.

Procedure 2-10 How to Log On as Administrator

1	Obtain the provisioning mode. See "Obtaining the Provisioning Mode" on page 2-13.
2	<p>To access the UNIX X Windows environment, do the following:</p> <ol style="list-style-type: none">1. Double-click the Preside Client Access icon on the client desktop. <p>Result: The CDE login page from the application server appears.</p> <ol style="list-style-type: none">2. In the Username field, type root and press Enter.3. In the Password field, type <root password> and press Enter.
3	To launch the application as administrator, type /opt/MagellanNMS/bin/nmstool Admin.tsets & and press Enter .
4	<p>From the Preside MDM main window, select System, and select Administration. Then select MDM Software Configuration.</p> <p>Result: The MDM Configuration, any Netscape error messages, Netscape:Config Help, and Netscape license agreement windows appear.</p>
5	Continue to Procedure 2-11.

Selecting the Network Type

Procedure 2-11 describes how to select the network type for the WAN switch.



NOTE

Ignore any fonts warning messages that appear during this procedure.

Procedure 2-11 How to Select the Network Type

1	At the Main menu, press 2 and press Enter to configure the MDM Subsystems. Result: The verifying licences for the packages...Press return to continue. message appears.
2	Press Enter . Result: The Network Type Selection menu appears.
3	Press 3 and press Enter for Network containing only Passport. Result: The Your network contains only Passport. Is this correct? prompt appears.
4	Press Y and press Enter . Result: The Base Package (1-11) menu appears.
5	Press 1 and press Enter for Passport Result: The Passport Access menu appears. Access.
6	Press 1 and press Enter for Create a new configuration. Result: The Passport Access (Create) menu appears.
7	Continue to Procedure 2-12.


Adding a WAN Switch for Preside MDM to Manage

Procedure 2-12 describes how to add a WAN switch for Preside MDM to manage.

Procedure 2-12 How to Add a WAN Switch for Preside MDM to Manage

1	At the Passport Access (Create) menu, press a and press Enter for Create a new member. Result: The Enter the group name for the new host prompt appears.
2	Type GST and press Enter for the group name for the new host.
3	Type <WAN Switch name > and press Enter for the name of the new host.
4	Type <the IP address of the WAN Switch> , for example, 10.1.233.51, and press Enter for the IP address. Result: The Would you like to save this entries? prompt appears.
5	Press Y and press Enter . Result: The Server (/opt/MagellanNMS/bin/fdtm) is already activated in the SVM list prompt appears.

Procedure 2-12 How to Add a WAN Switch for Preside MDM to Manage (Continued)

6	At the <code>Press carriage return to continue.</code> prompt, press Enter . Result: The Server (<code>/opt/MagellanNMS/bin/hgds</code>) is already activated in the SVM list prompt appears.
7	At the <code>Press carriage return to continue.</code> prompt, press Enter .
8	At the <code>Press carriage return to continue.</code> prompt, press Enter .
9	To add multiple WAN switches to be managed in the same or other zones, repeat steps 1 through 8. Keep the same settings except for the following: <ul style="list-style-type: none"> For <WAN Switch name>, enter a different name. For <the IP address of the WAN Switch>, enter a different IP (for example, "10.2.233.51") <p>If you are finished, continue to the next step.</p>
10	Press Q and press Enter until the Base Package list (1 to 11) appears.
11	Continue to press Q and press Enter to exit this menu and the Passport Access (Create) menu.
12	From the UNIX Xterm window, to enable the FMDR_GST server, type <code>/opt/MagellanNMS/bin/fmsgetmod -v <software version of the WAN switch> -u <IP address of the WAN Switch> <admin or mdmmgr username> <admin or mdmmgr password for the username></code> and press Enter .
13	Wait several minutes for the <code>#</code> prompt to appear. You can then type in the next zone and continue on for subsequent zones. (Example 1: <code>/opt/MagellanNMS/bin/fmsgetmod -v CD01C -u 10.1.233.51 mdmmgr <mdmmgr password></code>)
	 <div style="background-color: #00AEEF; color: white; padding: 5px; display: inline-block;">NOTE</div> <p>The software version "CD01C" in the above example is variable. Your software version may be this version or higher.</p>
14	Continue to Procedure 2-13.

Adding WAN Switches to the Configuration Files

Procedure 2-13 describes how to add the WAN switch to the configuration file.

Procedure 2-13 How to Add a WAN Switch to the Configuration File

1	<p>In the UNIX Xterm window, type crontab -e and press Enter.</p> <p>Result: A text editor file opens.</p>
2	<p>1. Arrow to the end of the file and find the following lines, for example:</p> <pre>0 0 * * 1-6 /opt/MagellanNMS/bin/cmcwrap /opt/MagellanNMS/bin/pbackup -pds presid1 mdmmgr <mdmmgr password> -auth GST mdmmgr <mdmmgr password> -target <WAN Switch name for zone 1> ...</pre> <p>2. Add the new WAN switch name at the end of the line.</p> <p>Result: The line now appears like the following:</p> <pre>0 0 * * 1-6 /opt/MagellanNMS/bin/cmcwrap /opt/MagellanNMS/bin/pbackup -pds presid1 mdmmgr <mdmmgr password> -auth GST mdmmgr <mdmmgr password> -target <WAN Switch name for zone 1> ...<new WAN Switch name> ...</pre> <div data-bbox="483 1039 586 1150"> </div> <div data-bbox="610 1066 844 1115"> <p>NOTE</p> </div> <p>Be careful with spacing. Add only one space between /pbackup and -pds and one space between <mdmmgr password> and -target. Also, you may have more WAN switches to add. The above example shows a two zone system.</p>
3	<p>From the File menu, select Save to save the file that you just typed, and then select Close.</p>
4	<p>From the UNIX Xterm window, type sync and press Enter.</p>
5	<p>Type init 6 and press Enter.</p> <p>Result: The workstation reboots.</p>
6	<p>Click Yes to dismiss the PC-Xware® dialog box.</p>
7	<p>Continue to Procedure 2-14.</p>

Verifying the WAN Switch Addition

Procedure 2-14 describes how to verify that the WAN switch was added correctly using Preside MDM and MDMWeb.

Procedure 2-14 How to Verify the WAN Switch Addition

1	<p>To access the UNIX X Windows environment after the server reboots, do the following:</p> <ol style="list-style-type: none"> 1. Double-click the Preside Client Access icon on the client desktop. <p>Result: The CDE login page from the application server appears.</p> <ol style="list-style-type: none"> 2. In the Username field, type mdmmgr and press Enter. 3. In the Password field, type <mdmmgr password> and press Enter. <p>Result: After approximately five minutes, the Welcome to Solaris screen appears, followed by the UNIX toolbar and Help Views window. You can minimize these windows, the Connects folder, and any additional console windows. Preside MDM automatically launches.</p>
2	<p>From automatically launched Preside MDM window, select Fault, and select Network Viewer.</p> <p>Result: The Network Viewer window appears. A window appears displaying "a new model ..."</p>
3	Click the load new model button.
4	<p>Double-click the icon(s) in the topology map.</p> <p>Result: The new added WAN switch icon appears in the topology map.</p>
5	<p>In the Network Viewer window, from the File menu, select Exit.</p> <p>Result: A window appears displaying "a new model ..."</p>
6	Click Exit and save .
7	Exit Preside MDM and CDE.
8	<p>Verify that the new WAN switch appears in MDMWeb.</p> <ol style="list-style-type: none"> 1. Access MDMWeb. See "Accessing MDMWeb" on page 2-50. Log on as mdmmgr. 2. In the navigation pane, verify that the new switch appears. See "Navigating in MDMWeb" on page 2-52. <p>Result: The new added WAN switch icon appears in the navigation pane.</p>

Connecting to the WAN Switch by Command Line



NOTE

To learn the UNIX commands used in the Command Console to communicate with the WAN switch, you must attend Nortel Passport training.

The Command Console is the user interface for communication between MDM and Passport. You can use a single instance of this tool to issue commands to multiple components for display purposes. The Command Console provides the same functionality provided by a local or remote text interface device.

Command Console provides the centralized flexibility for you to access the WAN switches by a command line interface.

You can perform the following tasks:

- Display
- List

For example, type **<WAN Switch name> d atmif/*** on the command line to show the configuration of the WAN switch.

Connecting to the WAN Switch Using Command Line Via Client Workstation

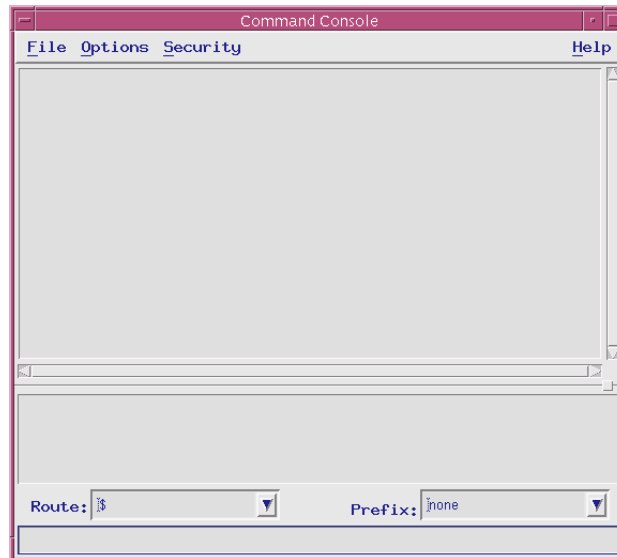
Procedure 2-15 describes how to connect to the WAN switch from the client workstation using the command line interface.

Procedure 2-15 How to Connect to the WAN Switch Using Command Line via Client Workstation

- 1 From the Preside MDM main window, click **System**, select **Utilities**, and then select **Command Console**.

Result: The Command Console window appears (Figure 2-18).

Figure 2-18 Command Console Window

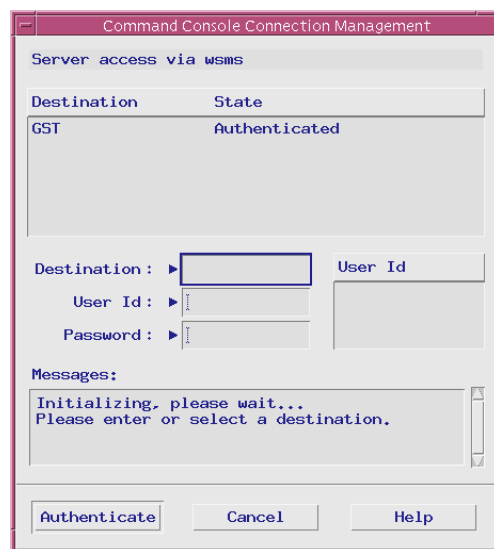


Procedure 2-15 How to Connect to the WAN Switch Using Command Line via Client Workstation (Continued)

2 From the Security menu, select **Connection Management**.

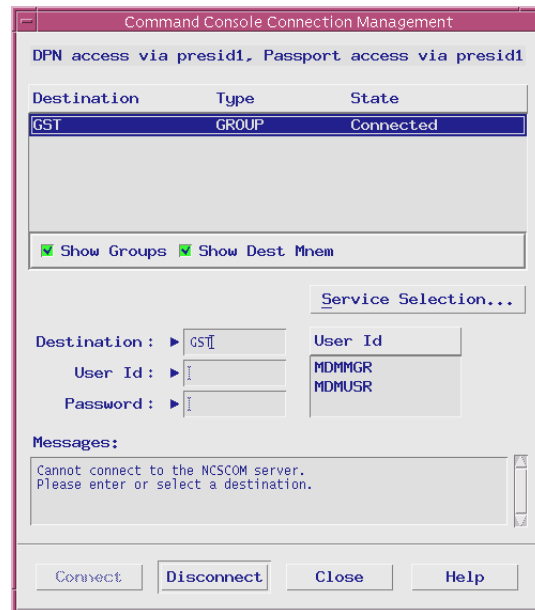
Result: The Command Console Connection Management dialog box appears (Figure 2-19).

Figure 2-19 Command Console Connection Management Dialog Box



Procedure 2-15 How to Connect to the WAN Switch Using Command Line via Client Workstation (Continued)

- 3** Select **GST**. In the User ID field, type **mdmusr** or **mdmmgr** (as applicable) and enter the password. Click **Connect** (Figure 2-19).

Figure 2-20 Command Console Connection Management Dialog Box

Result: After waiting five seconds, the **Connect** button becomes dimmed.

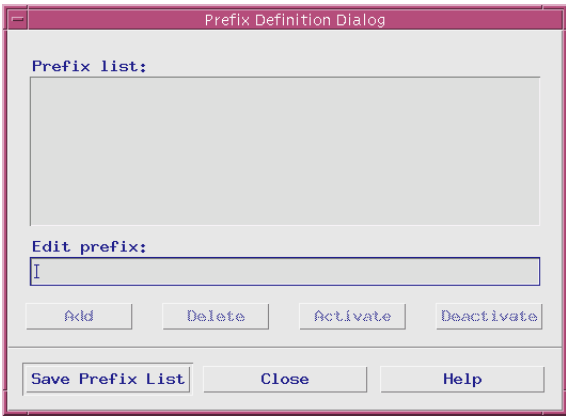
- 4** Click **Close** to close the Command Console Connection Management dialog box.

Result: The Command Console Connection Management dialog box closes.

Adding Prefixes

Text prefixes can be optionally added to WAN switches. This is useful in relating a WAN switch to an entity or object. Procedure 2-16 is a procedure that describes how (by an example) to add prefixes to help further identify a WAN switch.

Procedure 2-16 How to Add Prefixes

1	Connect to the WAN switch. See Procedure 2-15.
2	<p>On the Command Console window (Figure 2-18), from the Options menu, select Prefix definition.</p> <p>Result: The Prefix Definition dialog box appears (Figure 2-21).</p> <p>Figure 2-21 Prefix Definition Dialog Box</p> 
3	In the Edit Prefix field, type <WAN Switch name> for zone 1. Click Add , and repeat this step with <WAN Switch name> for zone 2, <WAN Switch name> for zone 3, and so on (depending on your system setup).
4	<p>Click Save Prefix List and click Close.</p> <p>Result: The Prefix Definition dialog closes.</p>
5	On the Command Console window (Figure 2-18), in the Route field, click on the down arrow and select GST .
6	<p>In the Prefix field, click on the down arrow and select 1.<WAN Switch name>.</p> <p>Result: Zone1 is automatically added to the front of the command input field.</p>
7	<p>In the command input field, after the zone1 prefix, type list and press Enter.</p> <p>Result: The Command Console window (Figure 2-18) displays a list of components under the WAN switch.</p>
8	Click Close to close the window.

Collecting and Displaying Performance Information

Use the Performance Viewer (PV) to collect and display performance information about traffic throughput on the WAN switch and CPU memory utilization. The PV application provides real-time statistics for WAN switch performance graphs of important statistical information to help determine the behavior of element components.



NOTE

InfoVista™ also provides performance data on the WAN switch for daily, weekly, monthly, and yearly periods. See Volume 5, for more information.

The PV provides the following capabilities:

- Helps trace faults in the network.
- Collects information about network load. With sufficient privilege, polling rate can be configured as 10 - 300 seconds.
- Generates statistics for reports and analysis.

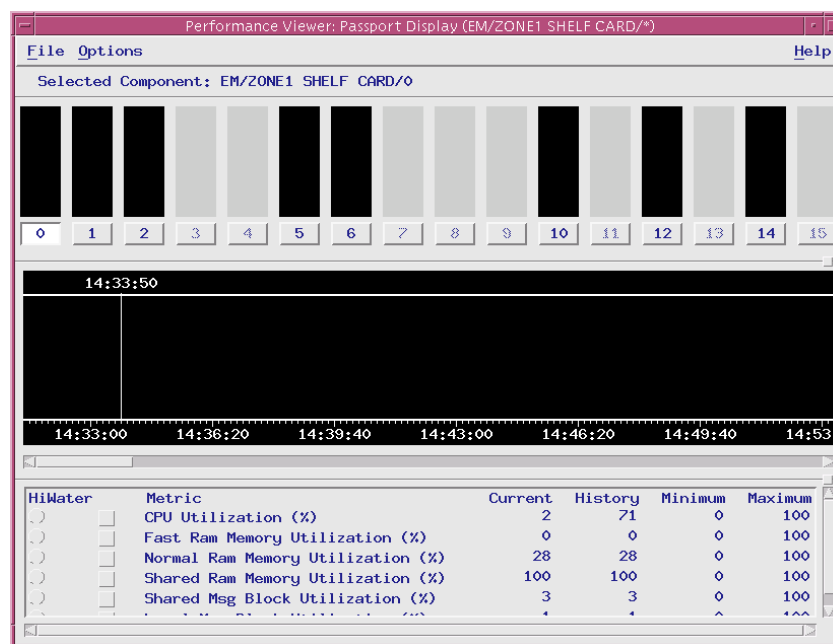
Procedure 2-17 describes how to collect and display performance information using the PV.

Procedure 2-17 How to Collect and Display Performance Information

1	<p>From the Preside MDM main window, click Performance, and select Passport/DPN Performance Viewer.</p> <p>Result: The Performance Viewer window appears.</p>
2	<p>From the Performance Viewer setup, set the Refresh Interval to 31 seconds.</p>
3	<p>In the Passport component field, type em/<WAN Switch name> shelf card/*.</p>
4	<p>Click OK.</p> <p>Result: The Performance Viewer Connection Management window appears.</p>
5	<p>Select GST, and enter your login name and password.</p> <ul style="list-style-type: none"> name: mdmmgr passwd: <mdmmgr password>

6	<p>Click Connect.</p> <p>Result: The Performance Viewer Connection Management window disappears and the Performance Viewer window appears (Figure 2-22).</p>
---	--

Figure 2-22 Performance Viewer Window

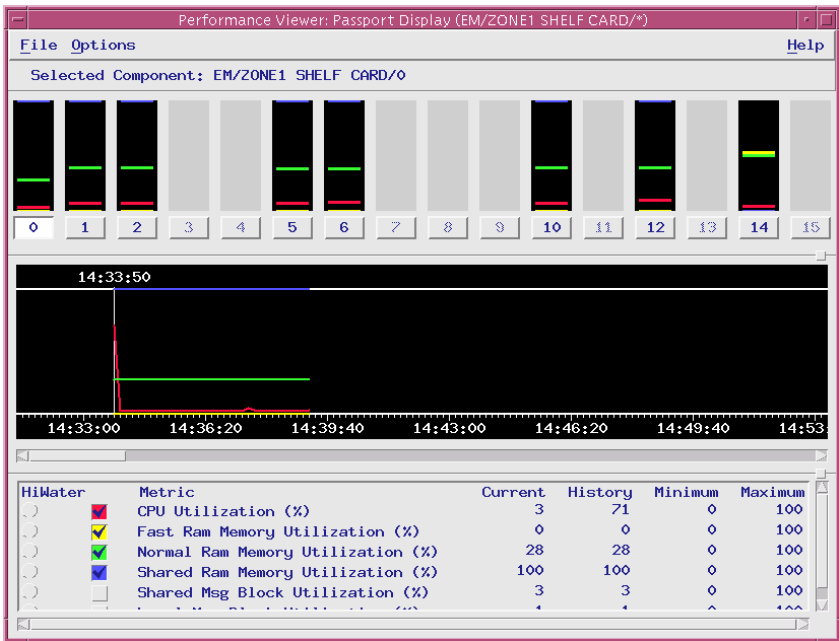


7	<p>In the Metric field, check the following:</p> <ul style="list-style-type: none"> CPU Utilization Fast Ram Memory Utilization Normal Ram Memory Utilization Shared Ram Memory Utilization
---	---

Procedure 2-17 How to Collect and Display Performance Information (Continued)

- 8
- In the Component field, click the **0** button, which represents card 0.
Result: The CPU and Memory performance information on card 0 appears (Figure 2-23).

Figure 2-23 Displayed CPU and Memory Performance for a Card



- 9
- From the Options menu, select **Change Parameters**.
Result: The Performance Viewer window reappears.

- 10
- In the Passport component field, type **em/<WAN Switch name> fruni/* dlci/***



NOTE

See "Useful Commands for Performance Viewer" on page 2-37 for more commands.

Procedure 2-17 How to Collect and Display Performance Information (Continued)

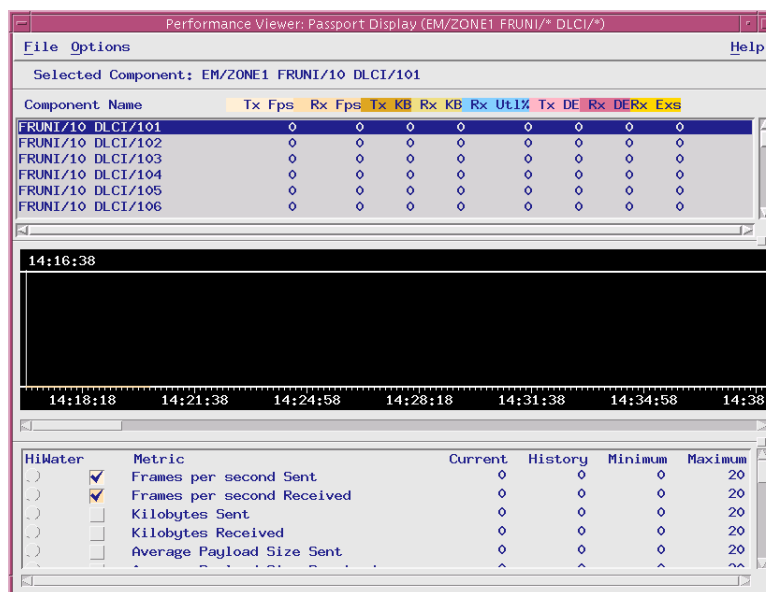
11 Click **OK**.

Result: The Traffic reports on each Fruni DLCI link appears. In the Metric field, select the following:

- **Frames per second Sent**
- **Frames per second Received**

Result: The Fruni DLCI Links Traffic Report appears (Figure 2-24).

Figure 2-24 Traffic Report



12 From the File menu, select **Exit** to close the window.

Useful Commands for Performance Viewer



NOTE

See the Preside CD ROM: Preside MDM for all valid Performance Viewer commands and for more information.

The following list shows useful commands for the Performance Viewer:

- EM/<WAN Switch name> SHELF CARD/*
- EM/<WAN Switch name> LP/*
- EM/<WAN Switch name> LP/* DS1/*

- EM/<WAN Switch name> LP/* E1/*
- EM/<WAN Switch name> FRUNI/*
- EM/<WAN Switch name> FRUNI/* LMI/*
- EM/<WAN Switch name> FRUNI/* FRAMER
- EM/<WAN Switch name> FRUNI/* DLCI/*
- EM/<WAN Switch name> ATMIF/*
- EM/<WAN Switch name> ATMIF/* VCC/*



NOTE

If you type in a command and a message appears as the result that indicates a failure to connect to the component, carefully re-type the command and try again. Do not try to modify the command as a shortcut.

Viewing the Status of WAN Switch Components

The Network Viewer (NV) displays a real-time graphic network map that shows the status of the WAN switch components on the network. The NV provides the following:

- Represents different node types by the shape of an icon and represents the states of components by the color of the icon.
- Displays views at different levels of detail. High-level view provides a view of the network offering quick identification of areas that require action.
- Improves the displayed information with Alarm Display's complete filtering capabilities. You can display module subcomponents down to the port level to trace a high-level problem to its source.
- Displays different levels of the network at the same time (for example, regional, site, and module levels).

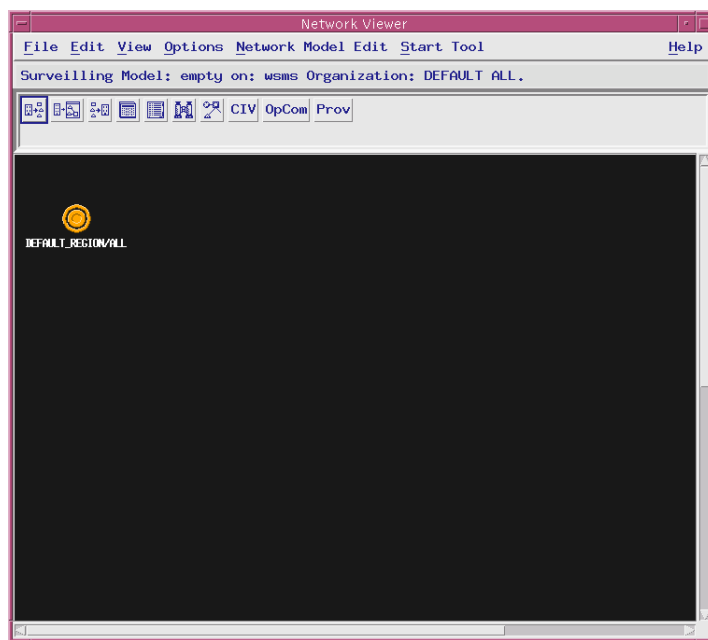
Procedure 2-18 describes how to check the status of a WAN switch component on the network.

Procedure 2-18 How to Check the Status of a WAN Switch Component

- 1 From the Preside MDM window, click **Fault**, and then select **Network Viewer**.

Result: The Network Viewer window appears (Figure 2-25).

Figure 2-25 Network Viewer Window



- 2 From the Options menu, select **Show all node labels** (if they are not already showing).



NOTE

The selection option indicates **Hide** instead of **Show** if the default display shows all node labels.

Result: The label of each node appears.

Procedure 2-18 How to Check the Status of a WAN Switch Component (Continued)

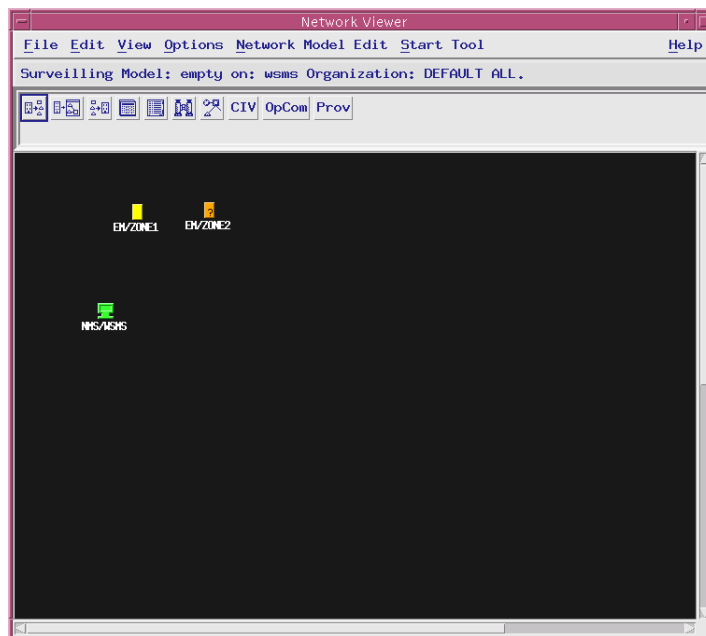
- 3** From the Network Viewer window, double-click **Default Region**, then double-click **Default Site**.

Result: The switch level appears (Figure 2-26).

**NOTE**

You can only perform fault management on the Passport devices, shown below as EM/ZONE1 and EM/ZONE2. If necessary, you can re-position the icons to avoid overlap.

Figure 2-26 Switch Level View



Procedure 2-18 How to Check the Status of a WAN Switch Component (Continued)

- 4** Select a switch type, EM/<**WAN Switch name**>, right-click, hold the mouse button down, and select **show shelf**.

Result: The status of logical shelf cards on the switch appears (Figure 2-27).

Figure 2-27 Status Dialog Box



- 5** The color on the graph indicates the status of the components. If you are unsure what the color status indicates, on the Network Viewer window, select **Legend** from the Options menu to check the color definition.

- 6** Click **Close** to exit the graph.

Accessing Component Information Viewer

The Component Information Viewer (CIV) provides you with detailed information about components and subcomponents of a network element. The CIV provides this information in text format. The CIV gathers state-, alarm-, and problem-based monitoring into one tool.

Use the CIV to perform the following tasks:

- Identify the component with the fault and any of its related components.
- Determine the effect of these faults.
- View the current state and problem state of these components.
- View the alarms and status received from these components.
- Execute diagnostic commands.

Procedure 2-19 describes how to access the CIV.

Procedure 2-19 How to Access the Component Information Viewer

- 1

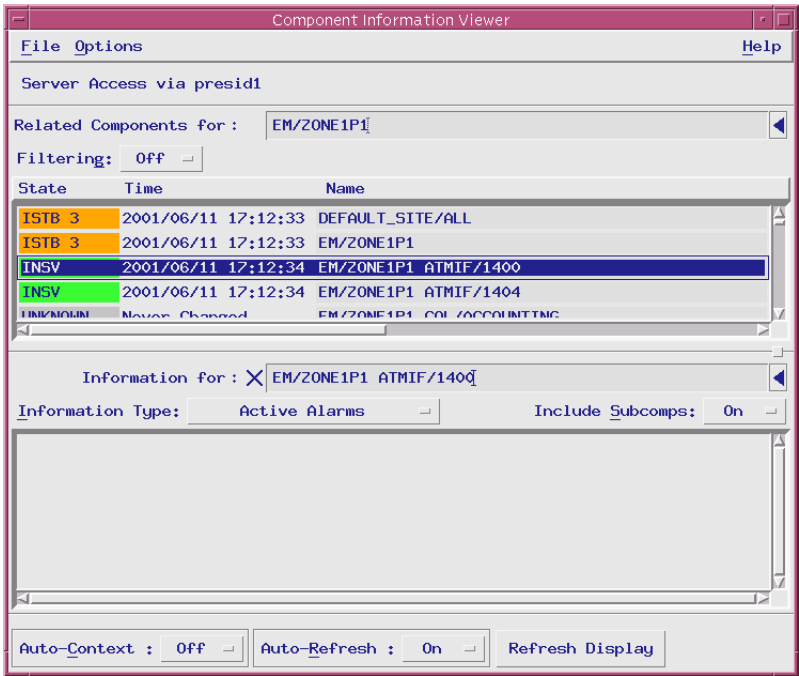
From the Preside MDM main window, click **Fault** and then select **Component Information Viewer**.

Result: The Component Information Viewer window appears (see Figure 2-28 for an example of the window).
- 2

In the **Related Components for** field, type **EM/<WAN switch name>** and press **Enter**.

Result: All the components and their statuses appear below the State, Time, and Name columns (Figure 2-28).

Figure 2-28 Component Information Viewer Window



- 3

From the File menu, select **Exit** to close the window.

Displaying WAN Switch Alarms

This section describes two methods to view alarm information about the WAN switch:

- HP OpenView

- Preside MDM Alarm Display

Displaying Alarms Using HP OpenView

The following section describes how you can also display alarm information and traps for the WAN switch using HP OpenView. HP OpenView provides the following alarm display information:

- **Passport Alarm Alarms category** — accesses an Alarms Browser window where you can view Nortel-provided traps.
- **Internet submap** — shows the WAN switch IP interface.
- **Default traps** — provides Nortel WAN switch trap definitions that are integrated with HP OpenView.



NOTE

See Volume 2, *Fault Management* for more information about displaying alarms on the WAN switch and viewing the WAN switch trap definitions. See **FullVision INM Online Help** for more information about displaying alarms.

Displaying Alarms using Preside

Alarm Display is the Preside MDM application for network fault management. You can detect, analyze, and correct network faults or degradation conditions (such as failures on cables, cards, and software links for the WAN switch). Alarm Display allows you to manage traps.

You can access Alarm Display from the client or MDMWeb (see "Displaying Alarms Using MDMWeb " on page 2-55).


Procedure 2-20 describes how to display alarms on the WAN switch using Preside’s Alarm Display client feature.

Procedure 2-20 How to View Alarms on the WAN Switch

1

From the Preside MDM main window, click **Fault**, and then select **Alarm Display: Active**.

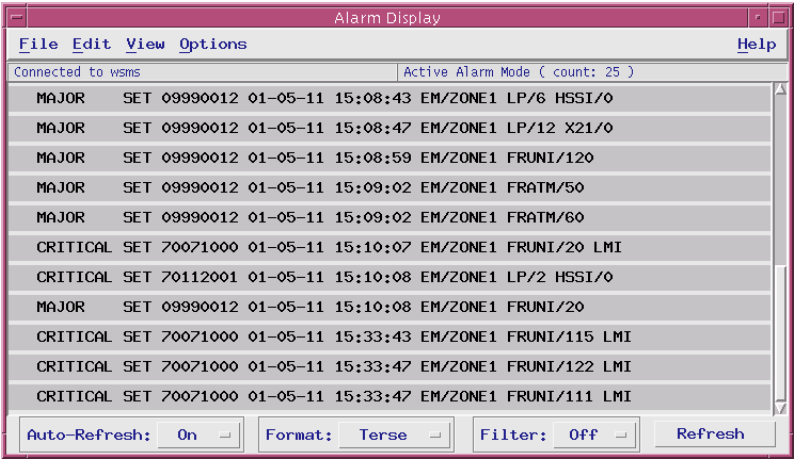
Result: The Alarm Display window appears (Figure 2-29).Notice that the first column shows the status of the components as Major or Critical, based on traps received from the WAN switch.



NOTE

Preside MDMWeb provides a detailed explanation of the alarm type in Alarm Display.

Figure 2-29 Alarm Display Window



2

As problems are solved, the traps disappear from the Alarm Display window. To see a log of past traps, from the Preside MDM main window click **Fault** and then select **Alarm Display: Log**. The Alarm Display log mode window appears. Using this step, you can locate alarms that have cleared from the Alarm Display window.)

3

From the File menu, select **Exit** to close the window.

Using Preside MDM for Fault Management

You can reset a card on the WAN switch to perform fault management tasks. Use this procedure, for example, if a Logical Processor is not performing and you want to switch over to a secondary card.

**IMPORTANT**

You must contact Motorola System Support Center (SSC) before attempting this procedure as it may impact system performance.

Resetting a Card on the WAN Switch

**CAUTION**

Do not reset the entire WAN switch as a whole. Doing so will cause problems in the network. Only cards should be reset.

**NOTE**

Only mdmmgr users can perform the reset command.

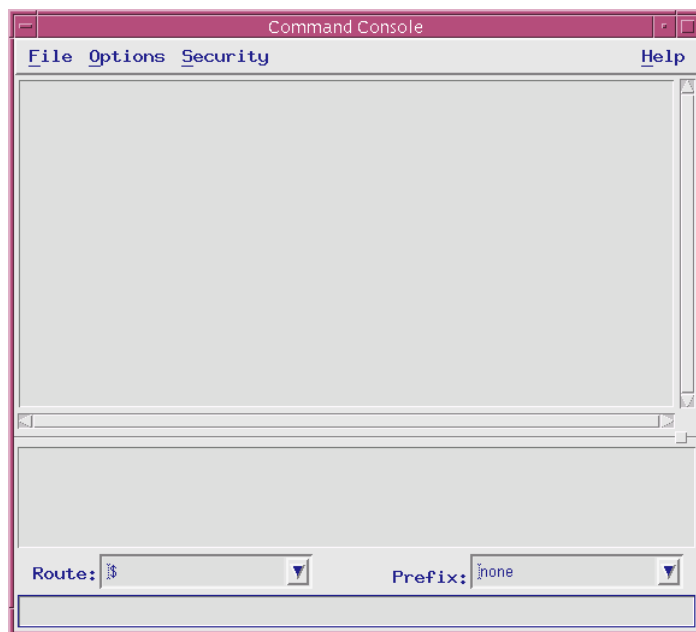
Procedure 2-21 describes how to reset a card on the WAN switch. Individual ports on a card, as well as the entire card, can be reset.

Procedure 2-21 How to Reset a Card on the WAN Switch

- 1 Connect to the WAN switch. See Procedure 2-15, "How to Connect to the WAN Switch Using Command Line via Client Workstation," on page 2-29.

Result: The Command Console window appears (Figure 2-30).

Figure 2-30 Command Console Window



- 2 In the Route field, click on the down arrow and select **GST**.
- 3 In the Prefix field, click on the down arrow and select **1.<WAN Switch name>**.
Result: <WAN Switch name> is automatically added to the front of the command input field.
- 4 In the command input field, after the zone1 prefix, type **list** and press **Enter**.
Result: The Command Console window (Figure 2-30) displays a list of components under the WAN switch.
- 5 To reset a card on the WAN switch, type **reset lp/<card number>** For example:
reset lp/3



IMPORTANT

Never reset the card/0; it reboots the entire WAN switch.

- 6 From the File menu, select **Exit** to close the window.

Using the MDMWeb



This section describes MDMWeb, describes how to access the application, and provides tasks you can perform.

Overview of MDMWeb

MDMWeb is a part of the Preside MDM software package that allows you to perform fault management tasks from the web browser. MDMWeb has more limited functionality than Preside MDM, but offers convenient multiple web access for remote users or workstations without PC-Xware.

MDMWeb additionally allows you to browse Nortel Networks Technical Publications.

Using a common desktop environment and a Web browser, the MDMWeb server software runs on Solaris. However, the MDMWeb client software runs on multiple platforms including Solaris and Windows 2000.

Menu Options

Table 2-6 shows the options available from MDMWeb. Menu options marked with an asterisk (*) are covered in this booklet. For procedures related to the unmarked menu options or for descriptions of the menu options, see the **MDMWeb Online Documentation**, available from the Help menu.

Table 2-6 MDMWeb Menu Options

Menu Option	Sub Menu Option	Description
Fault	Network Browser	Starts the network browser application. The network browser application displays network element states and allows you to navigate the network hierarchy.
	Alarm Display*	Starts the alarm display application. The alarm display application displays alarms in the network, either in active alarm mode or in alarm log mode.
	Network Status	Starts the network status application. The network status application provides a high-level view of the network status including component states. Network Status lets you know how many WAN switches are in your system and how many alarms.
	Troubled Components	Shows troubled components on the switch.
	Component Information Viewer	Starts the component information viewer application. The component information viewer application provides state and alarm information for a specified component.
System	Administration	Accesses the following commands: <ul style="list-style-type: none"> • Server Status Display • System Log Display • Connection Management • Prefix Editor
	Utilities*	Accesses the Command Console command. The command console application establishes a group connection and directly accesses the network device to allow command input.

Table 2-6 MDMWeb Menu Options (Continued)

Menu Option	Sub Menu Option	Description
Options	Change Look & Feel	Changes the look and feel of the platform. By default, the MDMWeb desktop opens with the Java Metal look and feel. Selecting the Change Look & Feel command toggles between the two choices for look and feel.
	Color Scheme	Selects one of the two color schemes for state and alarm information: <ul style="list-style-type: none"> MDM Color Scheme Standard Color Scheme
Window	Cascade	Aligns the open application windows so that they cascade from the top left corner.
Help	About MDMWeb	Displays information about the MDMWeb application.
	Online Documentation	Displays the online help. Use Online Documentation to access information about the dialog boxes and their menu options.
File	Exit	Closes the MDMWeb session. When you select this command from a client applet, MDMWeb shuts down its server connections and the MDMWeb display stops working.
	Alarm Display*	Starts the alarm display application. The alarm display application displays alarms in the network, either in active alarm mode or in alarm log mode.

Access Points for MDMWeb

You can access MDMWeb from either the NM or TNM client as follows:

- **NM Access:** From the Start menu, select **Programs**, select **Transport Network Management Applications**, select **WAN Switch Management Server**, and then select **Preside WAN Mngmt Web Access** (Figure 2-31).

Figure 2-31 Transport Network Management Applications Menu

- **TNM Client Access:** From the client desktop, double-click the **Preside Web Access** icon (Figure 2-32).

Figure 2-32 Desktop Icon



Accessing MDMWeb

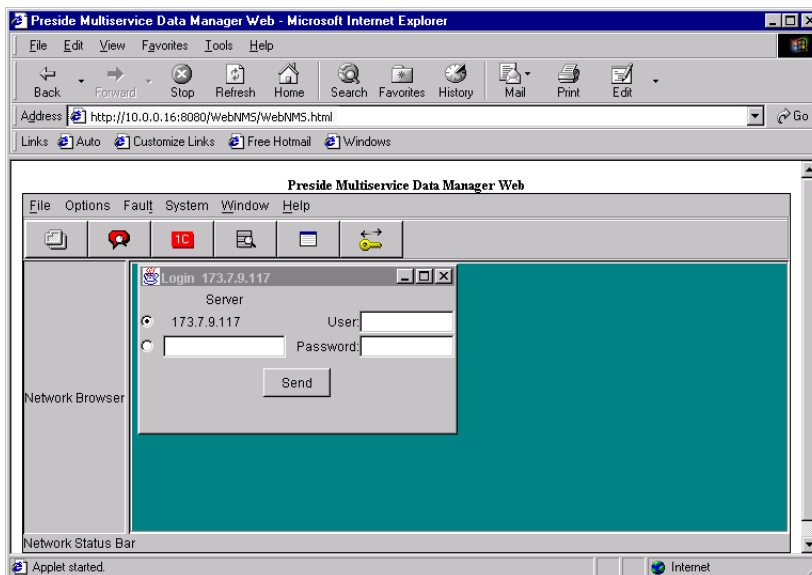
Procedure 2-22 describes how to access the MDMWeb application. If you have problems accessing MDMWeb, see Procedure 2-22.

Procedure 2-22 How to Access the MDMWeb

- 1 Double-click the **Preside Web Access** icon on the desktop.

Result: The MDMWeb login page appears (Figure 2-33).

Figure 2-33 MDMWeb Login Page

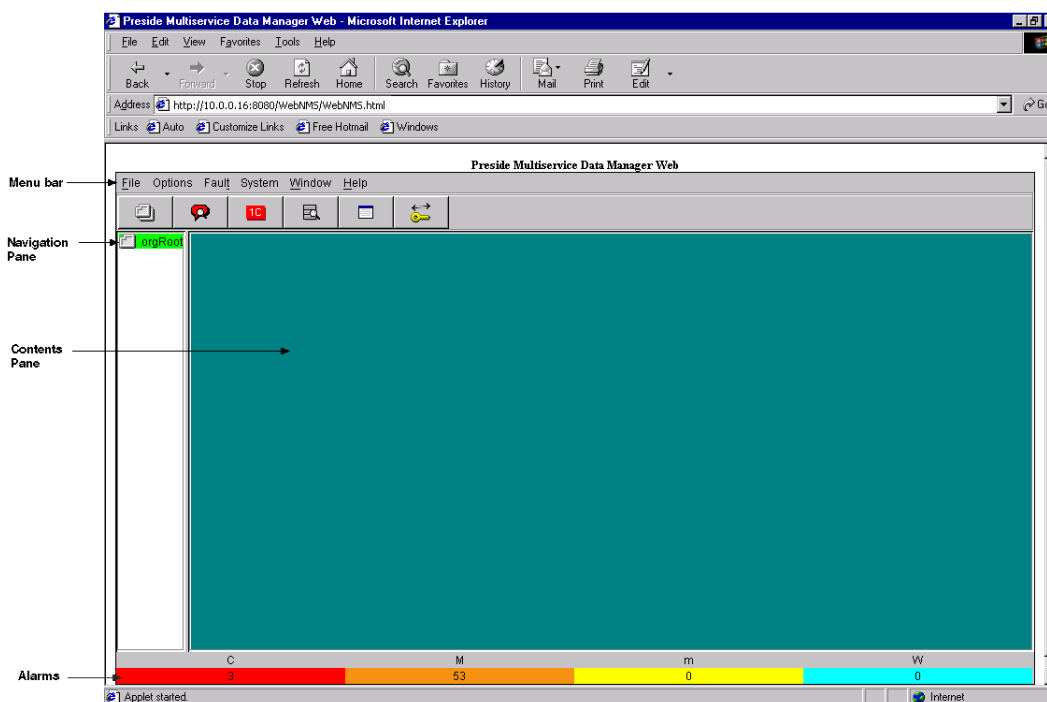


Procedure 2-22 How to Access the MDMWeb (Continued)

- 2** Enter your user name (**mdmusr** or **mdmmgr**, as applicable) and password and click **Send**.

Result: The MDMWeb Main page appears (Figure 2-34). The labeled elements show the parts of the main page, the menu bar, navigation pane, and contents pane.

Figure 2-34 MDMWeb Main Page



Navigating in MDMWeb

Procedure 2-23 describes how to navigate in MDMWeb. You use MDMWeb to view the switch data or configuration when using the web browser is more convenient than using Preside MDM.

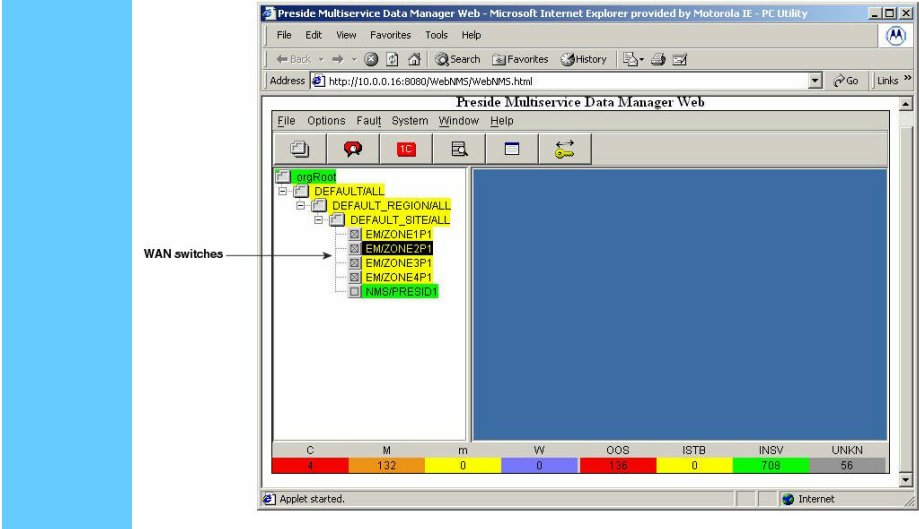
Procedure 2-23 How to Navigate to Display the Managed Switches

- 1

In the Navigation pane, double-click **OrgRoot**, then double-click **Default/ALL**.
Result: The navigation pane expands.
-
- 2

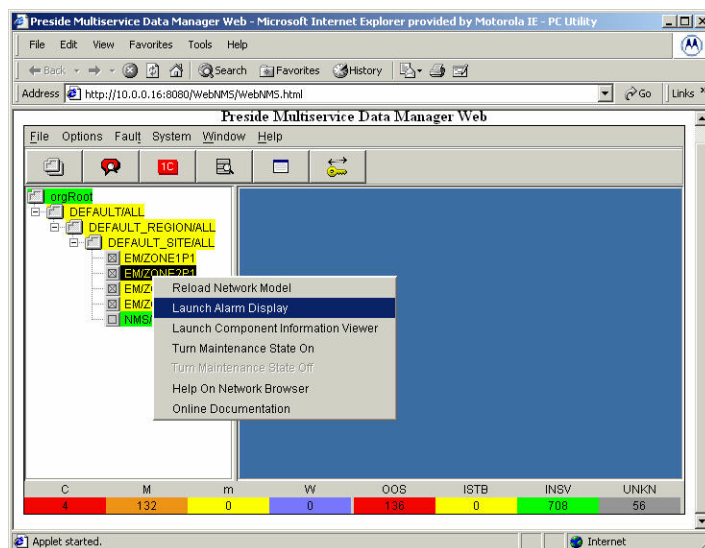
Double-click **Default Region/ALL**, then double-click **Default Site/ALL**.
Result: All managed WAN switches appear in the navigation pane (Figure 2-35).

Figure 2-35 View of Managed WAN Switches in MDMWeb



Procedure 2-23 How to Navigate to Display the Managed Switches (Continued)

- 3** Access information for a particular switch by right-clicking on the switch. Select an option from the pop-up menu, as desired (Figure 2-36).

Figure 2-36 Pop-Up Menu Available from Navigation Pane**How to Correct Access Problems (Example Procedure)**

Procedure 2-24 describes how (by example) to correct a common access problem by verifying that the proxy server setting was disabled.

Procedure 2-24 How to Correct Access Problems

- | | |
|----------|---|
| 1 | On the Microsoft® Internet Explorer window, from the Tools menu, select Internet Options .

Result: The Internet Options dialog box appears. |
| 2 | Select the Connections tab, then click LAN settings . |
| 3 | Clear the Use a proxy server check box. |
| 4 | Click OK to save the change and then click OK again to exit the window. |
| 5 | Enter the URL for MDMWeb. (The URL is http://10.0.0.16:8080/Web-NMS/WebNMS.html if you want to bookmark it.) |

Connecting to the WAN Switch Using Command Line Via MDMWeb

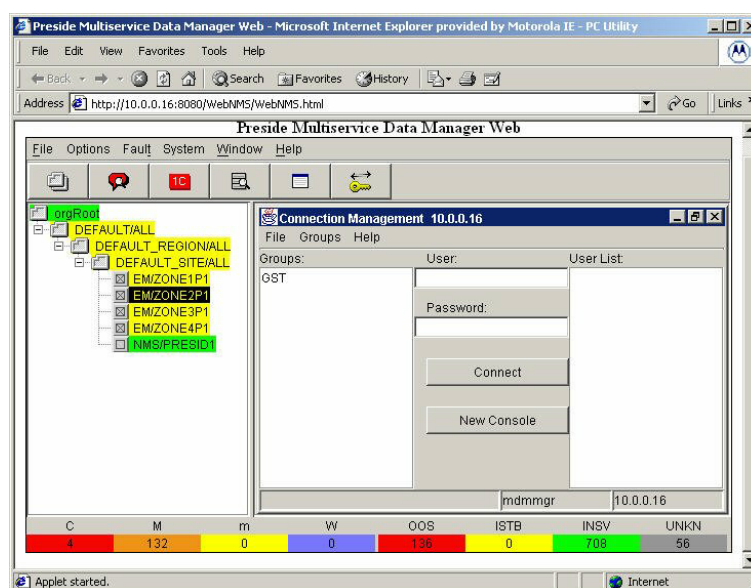
Procedure 2-25 describes how to connect to the WAN switch using the command line. Access from the command line using MDMWeb is more limited than the client interface. The user logon

defines the privileges: mdmmgr has full access to the switch, mdmusr has view only access. (The privileges are the same as the regular Preside MDM logons.)

Procedure 2-25 How to Connect to the WAN Switch Using Command Line Via MDMWeb

- 1 From the System menu, select **Utilities**, and then select **Command Console**. (Figure 2-34).
Result: The Command Console window appears in the contents pane.
- 2 On the Command Console window, from the Security menu, select **Connection Management**.
Result: The Connection Management window appears (Figure 2-37).

Figure 2-37 Connection Management Window



- 3 Wait 5 seconds. Select **GST** and then type your user name and password. Click **Connect**.
- 4 Wait a few seconds, and the **Connect** button label changes to **Disconnect**.
- 5 From the File menu, select **Close** to close the Connection Management window.
- 6 Continue to Figure 2-22.

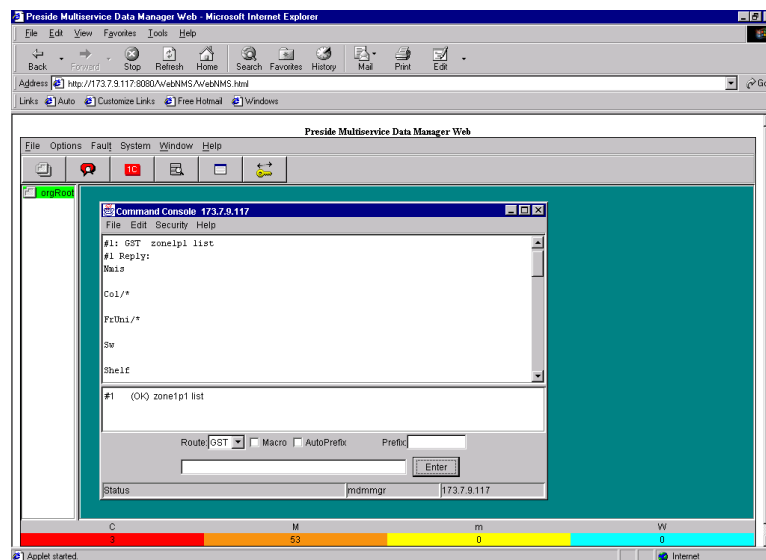
Displaying a Component List for the WAN Switch (Example Procedure)

Procedure 2-26 is an example procedure that describes how to display a component list for the WAN switch.

Procedure 2-26 How to Display a Component List for the WAN Switch

- 1 From the Command Console window, in the Route drop-down list, click on the down arrow and select **GST**.
- 2 From the command line field, type **<WAN Switch name> list** and press **Enter**.
Result: The component list at the WAN switch, **<WAN Switch name>**, appears (Figure 2-38).

Figure 2-38 Component List for the WAN Switch



- 3 From the File menu, select **Exit** to close the window.

Displaying Alarms Using MDMWeb

This section describes how to use MDMWeb to display alarms.

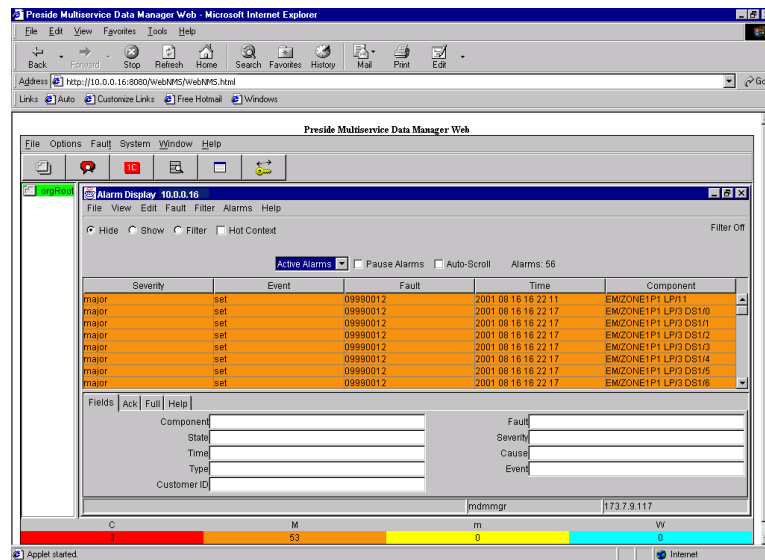
- Procedure 2-27 shows an example using the Fault menu and selecting **Active Alarms** to view all active alarms.
- Procedure 2-28 shows an example using the Alarm Display window and viewing alarms by alarm severity.

Displaying Alarms Using MDMWeb (View all Active Alarms)

Procedure 2-27 describes how to use MDMWeb to display alarms using the Fault menu and selecting **Active Alarms** to view all active alarms.

Procedure 2-27 How to Display Alarms Using MDMWeb (View all Active Alarms)

- 1** From the **Fault** menu (Figure 2-34), select **Alarm Display**.
Result: The Alarm Display window appears displaying the Alarm Log page.
- 2** Select the **Hide** radio button to narrow the selection.
Result: The Alarm Display view changes depending on the radio button selection.
- 3** From the drop-down list, select **Active Alarms**.
Result: The active alarms appear (Figure 2-39). Alarms show the severity, fault, and the component generating the alarm.

Figure 2-39 Alarm Display Window (All Active Alarms)

- 4** Select an alarm and select the **Help** tab for an explanation of how the WAN switch generates the alarm.
Result: The Help window provides the alarm interpretation for the selected alarm.
- 5** From the File menu, select **Exit** to close the window.

Displaying Alarms Using MDMWeb (View Alarms by Severity)

Procedure 2-28 describes how to use MDMWeb to display alarms using the Alarm Display window to view alarms by alarm severity.

Procedure 2-28 How to Display Alarms Using MDMWeb (View Alarms by Severity)

- 1** From the Navigation pane, right-click a switch and select **Alarm Display** from the pop-up menu.
Result: The Alarm Display window appears displaying the Alarm Log page.

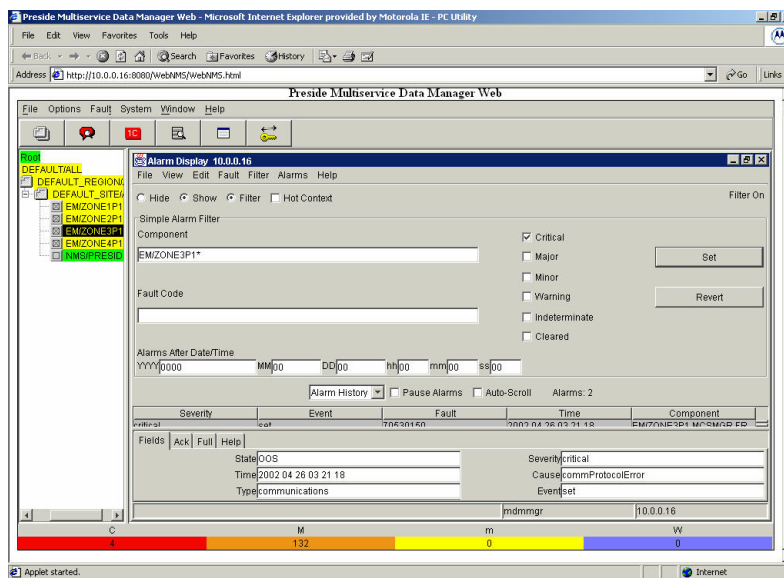
Procedure 2-28 How to Display Alarms Using MDMWeb (View Alarms by Severity) (Continued)

- 2** Narrow the display as desired, for example:
1. Select the **Show** and **Filter** radio button to narrow the selection.
 2. Choose an Alarm severity, for example, **Critical**.
 3. From the drop-down list, select **Alarm History**.

3 Click **Set**.

Result: The active alarms appear (Figure 2-40).

Figure 2-40 Alarm Display Window (Filtered by Severity)



- 4** Click an alarm to view.
- Result:** The **Fields** tab shows the alarm details (Figure 2-40).

- 5** Select an alarm and select the **Help** tab for an explanation of how the WAN switch generates the alarm.

Result: The Help window provides the alarm interpretation for the selected alarm.

- 6** From the File menu, select **Exit** to close the window.

This page intentionally left blank.

Managing the Routers

This chapter describes how to manage the routers in your system using the Router Manager User Interface (UI).

The Router Manager UI resides on the FullVision® Integrated Network Manager (INM) server. Router Manager enables you to group the routers so you can backup, restore, and reboot more than one router at a time. You can also use Router Manager to maintain router configuration and software files on the FullVision INM server and view router information, perform checksums, and launch WEBLink and Telnet sessions.

This chapter explains how to use Router Manager in your Motorola® system and includes the following topics:

- "Overview of Tasks" on page 3-1
- "Accessing the Router Manager UI" on page 3-5
- "Managing Groups" on page 3-7
- "Performing Router Management Functions" on page 3-13
- "Upgrading EOS Software on Routers in the Field" on page 3-40
- "Using the Portal to Upgrade EOS Firmware with Router Manager" on page 3-45
- "BCUB File Format" on page 3-54
- "Using WEBLink" on page 3-54

Overview of Tasks

Router Manager is a device management and grouping application that also operates as an HP® OpenView® plug-in. Use Router Manager to do the following:

- View a hierarchy of Motorola Network Router (MNR) S Series S4000 and Motorola Network Router (MNR) ST Series ST5000 routers (referred to generically as, MNR S Series and ST Series routers).
- Group routers in ways that make your management tasks easier, so that you can perform tasks on a group of routers, such as downloads and reboots.
- Back up and restore Router Manager data files. You can use this function to input new router sets. For details, see "Backing Up Router Manager Data Files on the FullVision INM Server" on page 3-21 and "Restoring Router Manager Data Files to the FullVision INM Server" on page 3-23.

- View runtime logs. For details, see "Viewing Runtime Logs" on page 3-18.

Applicable Management Tasks for Selected Routers or Groups

Table 3-1 lists the management tasks you can perform on selected routers or groups.

Table 3-1 Management Tasks

Tasks	Procedure in this chapter
Transfer files between routers and the FullVision INM server	"Downloading Files to Routers" on page 3-14 "Capturing (Uploading) Files From Routers" on page 3-16
Reboot routers	"Rebooting Routers" on page 3-25
Set reboot directories for routers	"Setting the Boot Block (Reboot Directory)" on page 3-32
Launch WEBLink or Telnet against routers	"Viewing Router Information and Launching Configuration Applications" on page 3-33
Perform checksums	"Performing Checksums" on page 3-37
View router information	"Viewing Router Information and Launching Configuration Applications" on page 3-33

Related Information in this Document Set

You can find other information about Router Manager or the routers managed by Router Manager using the following sources:

- **FullVision INM Online Help** — explains the MNR S Series and ST Series router topology maps available using HP OpenView and the HP OpenView Web Interface.
- Volume 2, *Fault Management*— Contains router trap definitions.
- **S Series S4000 Hardware User Guide** — provides instructions for installing a Motorola S Series S4000 router and performing basic device configuration.
- **ST5000 Series Hardware User Guide** — provides instructions for installing a Motorola ST5000 Series router and performing basic device configuration.
- **Enterprise OS Software User Guide** — provides information about how to use Enterprise OS (EOS) software to operate and configure your router.

- **Enterprise OS Software Reference Guide** — provides detailed information about commands and syntax for all EOS service parameters.

**NOTE**

If InfoVista™ is not purchased for your system, you must install Adobe® 4.05 from the system documentation set CD before you can view the EOS documentation. This documentation is available from the Help menu of the Router Manager UI, from the EOS Release CD, or from the WEBLink **Documentation** link.

**NOTE**

An ASTRO 25 SE system does not use InfoVista, Preside MDM, or CiscoWorks2000. Ignore all references to these software applications.

**NOTE**

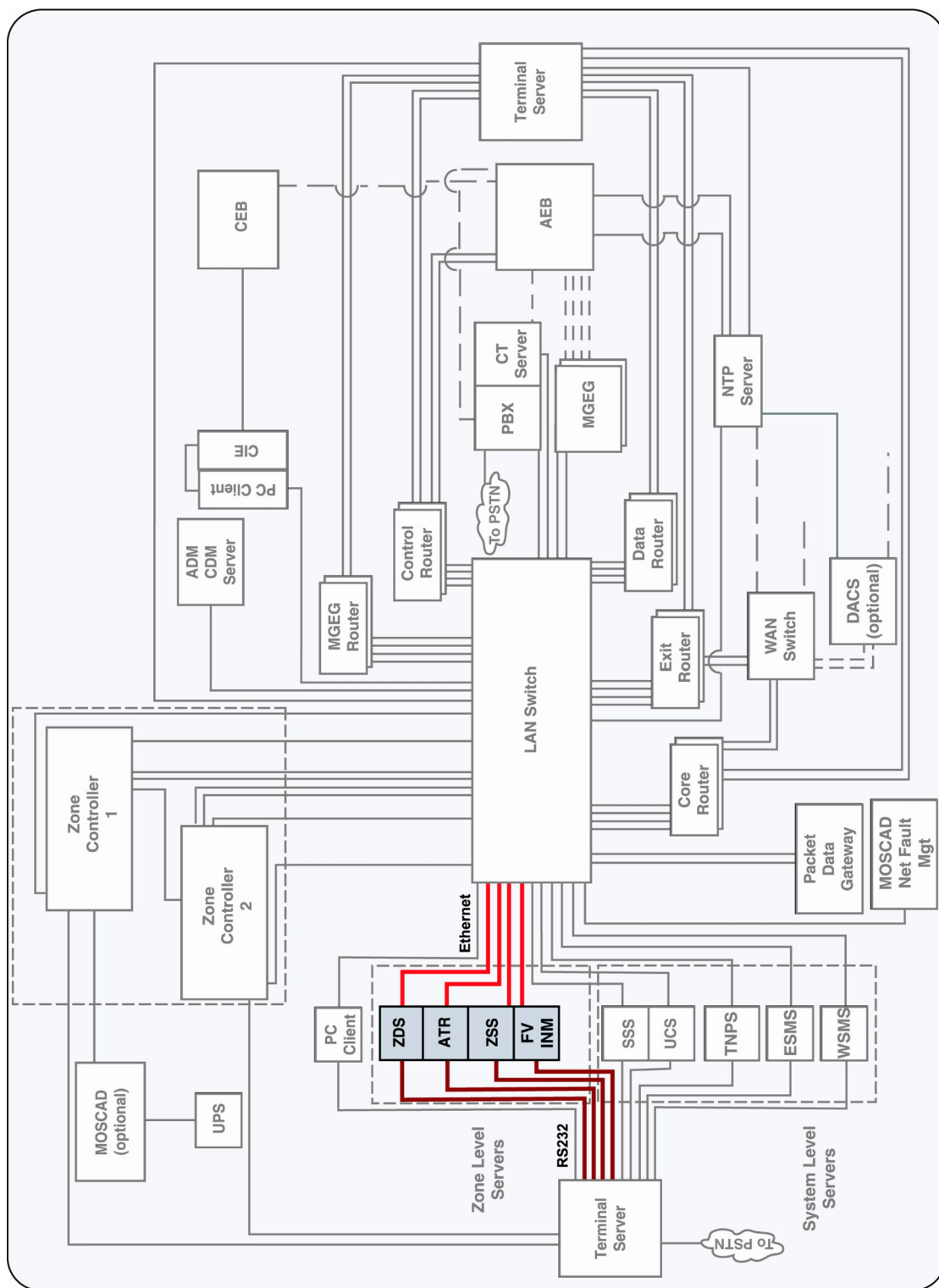
Router Manager does not provide the router EOS help file with the application, because the EOS help file content varies per EOS release. When Router Manager performs the software restore from Client to Server, a certified router EOS tar file includes the help file and automatically updates to the server. For the procedure of restoring the EOS tar file, see "Restoring Router Manager Data Files to the FullVision INM Server" on page 3-23.

System Diagram



Figure 3-1 shows how the FullVision INM server (where Router Manager resides) fits into the system Master Site.

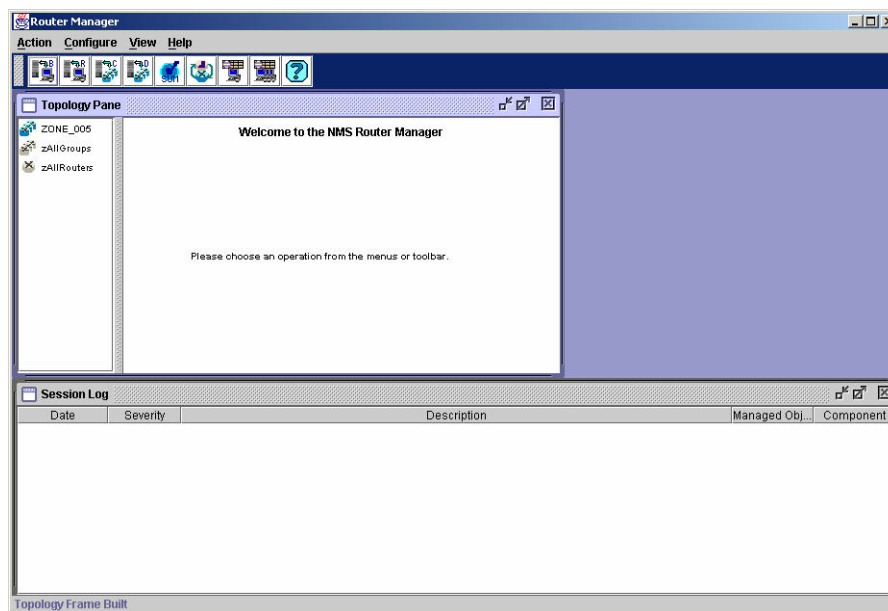
Figure 3-1 System Diagram Example



Accessing the Router Manager UI

You can access the Router Manager UI (Figure 3-2) from a Windows® 2000 Network Management (NM) client.

Figure 3-2 Router Manager Welcome Window



NOTE

To access the MNR S Series and ST Series routers topology maps on the FullVision INM server using HP OpenView and the Web HP OpenView, see the **FullVision INM Online Help**. For router trap definitions, see Volume 2: *Fault Management*.



NOTE

See Volume 1: *Understanding Your ASTRO 25 Trunking System* for the Application Launcher procedures.

Procedure 3-1 describes how to access Router Manager using the Application Launcher.

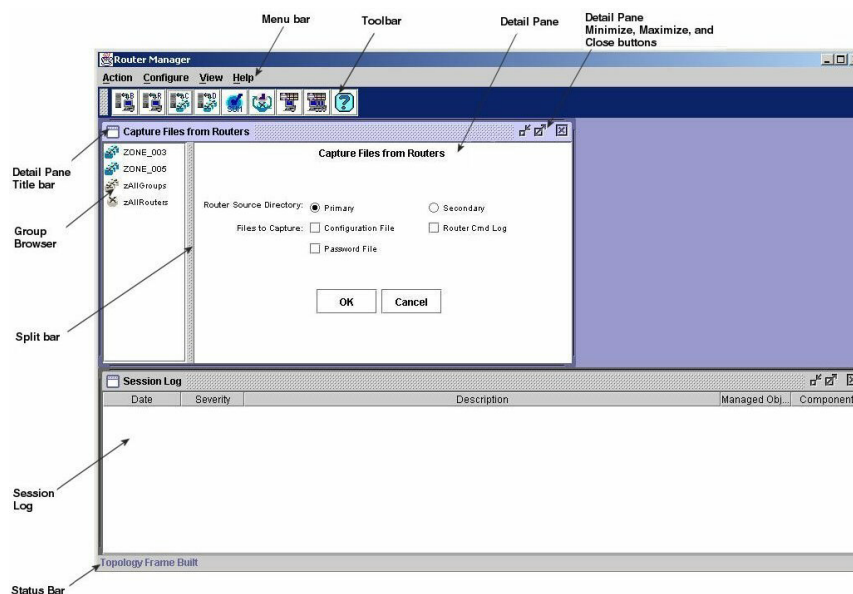
Procedure 3-1 How to Access Router Manager

1	Do one of the following to access the Router Manager UI:					
	<table border="1"> <thead> <tr> <th data-bbox="224 384 711 436">IF you want to:</th><th data-bbox="711 384 1427 436">THEN...</th></tr> </thead> <tbody> <tr> <td data-bbox="224 436 711 636">Access using the Private Radio Network Manager (PRNM) desktop icon:</td><td data-bbox="711 436 1427 636"> <ol style="list-style-type: none"> 1. Double-click the PRNM Suite Application Launcher desktop icon. 2. From the Windows Explorer window, select a zone folder, and then double-click Router Manager for the zone that you want to access. </td></tr> <tr> <td data-bbox="224 636 711 766">Access using the Motorola PRNM Suite Start menu:</td><td data-bbox="711 636 1427 766"> <ol style="list-style-type: none"> 1. From the Start button, select Motorola PRNM Suite. 2. Select a zone folder, and then click Router Manager for the zone that you want to access. </td></tr> </tbody> </table>	IF you want to:	THEN...	Access using the Private Radio Network Manager (PRNM) desktop icon:	<ol style="list-style-type: none"> 1. Double-click the PRNM Suite Application Launcher desktop icon. 2. From the Windows Explorer window, select a zone folder, and then double-click Router Manager for the zone that you want to access. 	Access using the Motorola PRNM Suite Start menu:
IF you want to:	THEN...					
Access using the Private Radio Network Manager (PRNM) desktop icon:	<ol style="list-style-type: none"> 1. Double-click the PRNM Suite Application Launcher desktop icon. 2. From the Windows Explorer window, select a zone folder, and then double-click Router Manager for the zone that you want to access. 					
Access using the Motorola PRNM Suite Start menu:	<ol style="list-style-type: none"> 1. From the Start button, select Motorola PRNM Suite. 2. Select a zone folder, and then click Router Manager for the zone that you want to access. 					

2	<p>Do one of the following:</p> <ul style="list-style-type: none"> • Select an option from the menu bar. • Select an option from the tool bar. • Browse the Group Browser.
----------	---

Figure 3-3 shows the elements of the Router Manager UI. (For information about how to use the features of the Router Manager UI, see **Router Manager Online Help**.)

Figure 3-3 Router Manager Main Window Elements



Logging Out of Router Manager

To log out of Router Manager, from the **Action** menu, select **Exit**.

Managing Groups



This chapter describes how to build default groups based on your network topology and describes how to add and delete routers.

Managing groups consists of the following tasks, which are individually discussed in this chapter:

- "Building Default Groups" on page 3-7
- "Adding and Deleting Routers" on page 3-9

Building Default Groups



IMPORTANT

This procedure is performed during the initial configuration. It is very unlikely that you ever need to add new groups. See Volume 9, *Master Site Hardware and Software Configuration* for more information.

When you launch Router Manager, the group browser is automatically populated with MNR S Series and ST Series routers known to HP OpenView. The routers are identified by their Sysnames (the system names assigned when the routers were configured) and placed into the pseudo group *zAllRouters*.

You can use the default group builder to place the routers into a hierarchy of groups based on their position in the topology: *Zone N*, *Zone N Site Routers*, *Zone N Core Routers*, and so on. Groups created by the default group builder are assigned read-only protection; you cannot rename or delete these groups and you cannot add routers and child groups to them.

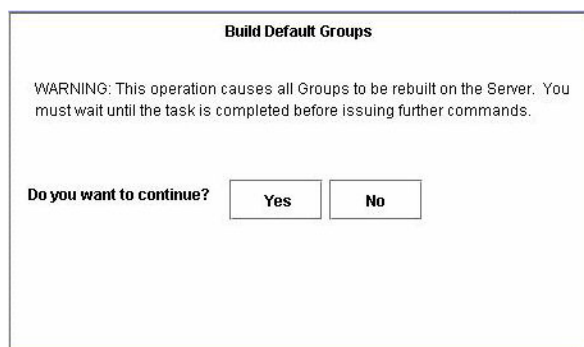
Procedure 3-2 describes how to build default groups.

Procedure 3-2 How to Build Default Default Groups

- 1 From the Router Manager Configure menu, select **Build Default Groups**.

Result: The Build Default Groups display appears (Figure 3-4).

Figure 3-4 Build Default Groups Display



- 2 Click **Yes** to build default groups. If default groups have already been built on the FullVision INM server, they are rebuilt when you issue this command.



CAUTION

You must wait until the default group building operation has finished before issuing further commands.

Figure 3-5 shows zone-level groups built in the group browser.

Figure 3-5 Default Groups in Group Browser

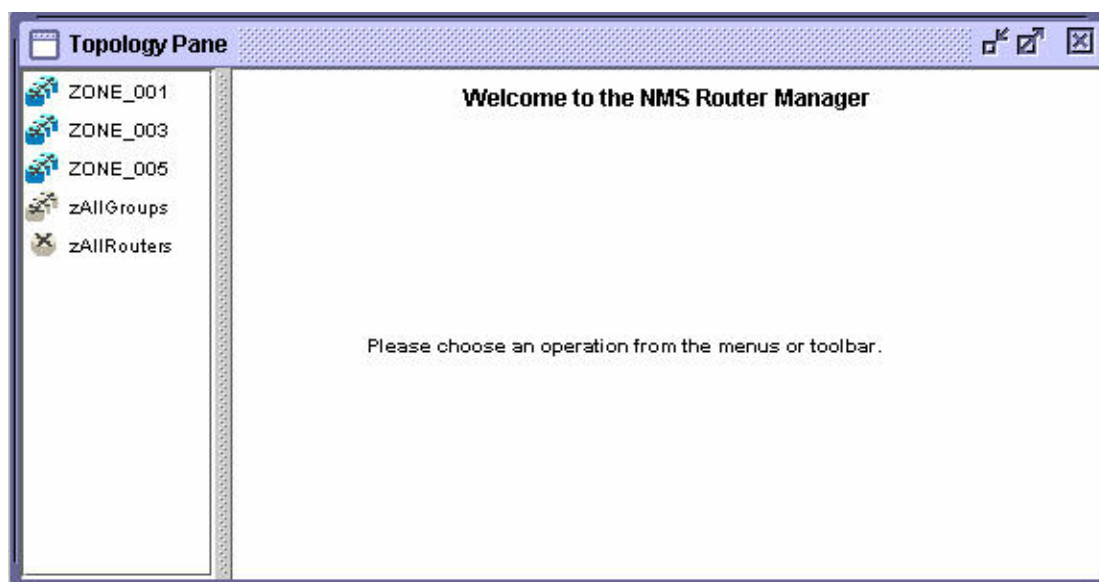
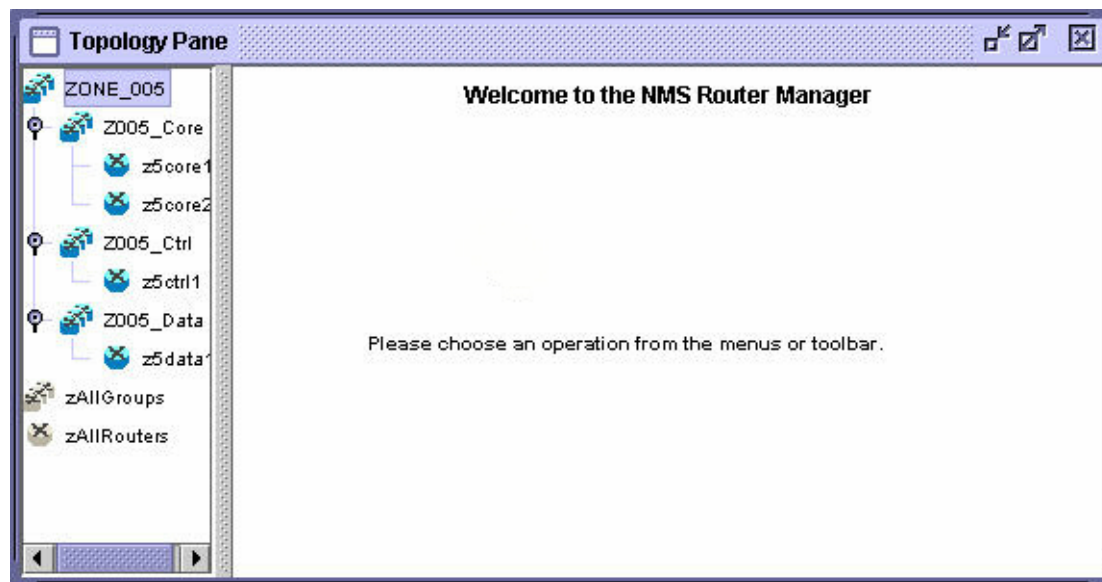


Figure 3-6 shows parts of the zone hierarchy expanded in the group browser. To expand the hierarchy, double-click groups icons.

Figure 3-6 Zone Groups with Parts of Hierarchy Expanded in Group Browser



Adding and Deleting Routers

This section describes how to prepare routers for management and how to add and delete routers from Router Manager.

Preparing the Routers for Management

Before you add a new router to Router Manager, make sure that the router is configured for management. Check the following:

- The router has been assigned an IP address.
For details about how to set the IP address for the MNR S Series and ST Series routers, see "Configuring a Basic IP Router" in the "Logging on and Performing Administrative Tasks" chapter of the appropriate hardware user guide.
- The router has been configured with routing information to the FullVision INM server.
For details about how to configure basic IP routing on the MNR S Series and ST Series routers, see "Configuring a Basic IP Router" in the "Logging on and Performing Administrative Tasks" chapter of the appropriate hardware user guide.
- The router has been assigned a system name (SysName) or a command to assign the router a system name exists in the boot.cfg file.
For details about how to assign a system name to the MNR S Series and ST Series routers, see "Setting System Information" in the "Logging on and Performing Administrative Tasks" chapter of the appropriate hardware user guide.

- The router is known to your network management platform with correct SNMP community strings. For details about how to set community strings for MNR S Series and ST Series routers, see the “SNMP Service Parameters” chapter of the *Enterprise OS Software Reference Guide*.
- An appropriate configuration (boot.cfg) file for the router resides on the FullVision INM server.



NOTE

You can also import a boot.cfg file from the Add Router display. For details, see "Adding Routers" on page 3-10.

- The router boot blocks are configured.
You configure the router boot blocks using the CLI **SysconF** command menus. For details, see the “Using the SysconF Menus” appendix in the appropriate hardware user guide. The boot block settings should be as follows:
 - Primary Boot Source: a:/primary/boot.ppc, a:/primary
 - Secondary Boot Source: a:/secondar/boot.ppc, a:/secondar
 - Test Boot Source: a:/primary/boot.ppc, a:/primary
 - Boot Sources: Primary and Secondary



NOTE

You cannot configure the router boot blocks via commands in the router’s boot.cfg file.

- Optimally, the router has been assigned an FTP username and password.

Sample Router Configuration

The following example configures a router with public and private community strings and a port with access to an FullVision INM server at IP address 10.1.233.10:

```
setd !2 -ip net=10.1.233.10 255.255.255.0
add -ip ro 0.0.0.0 10.1.233.1 9
setd -snmp control=trap
add -snmp comm "<read community string> RW ALL
add -snmp manager <read community string> 10.1.233.10 "ALL"
add -snmp comm <write community string> RO ALL
```

Adding Routers

Any router you add is automatically placed in the *zAllRouters* pseudo group.

Procedure 3-3 describes how to add a router to Router Manager.

Procedure 3-3 How to Add a Router

- 1** From the Configure menu, select **Add Router**.
Result: The Add Router display appears (Figure 3-7).

Figure 3-7 Router Manager Add Router Display

- 2** In the Router SysName field, enter the router's system name.

- 3** In the Router IP Address field, enter the router's IP address.



NOTE

It is recommended that you use the router's system IP address. However, if the router does not have a system IP address you can use the IP address of one of the router's Ethernet interfaces.

- 4** Optionally, in the Router Configuration File field, enter the path and filename for the router's configuration (boot.cfg) file. You can also use the **Browse** button to browse to the appropriate configuration file. When you add a configuration file with the router, this file is then available on the FullVision INM server and can be downloaded to other routers.



NOTE

Another way to obtain a boot.cfg file is to add a router without a Router Configuration File, then use the Capture display to upload the boot.cfg file from the router. For details, see "Capturing (Uploading) Files From Routers" on page 3-16.

- 5** Click **OK**.
Result: A confirmation dialog box appears, listing the system name and IP address of the router you are adding and the group to which it will be added (by default, the **zAllRouters** group).
- 6** Verify the information in the confirmation dialog box, then click **OK** to add the router.

Deleting Routers

Procedure 3-4 describes how to delete a router from Router Manager.



You can delete only one router at a time.

Procedure 3-4 How to Delete a Router

1	In the group browser, select the router you want to delete.
2	<div>From the View menu, select Router.</div> <div>Result: The View Router display appears (Figure 3-8).</div>
<div>Figure 3-8 Router Manager View Router Display</div> <div></div>	
For details about using the View Router display, see "Viewing Router Information and Launching Configuration Applications" on page 3-33.	
3	<div>Click Delete Router.</div> <div>Result: A confirmation dialog box appears, listing the system name of the router you are deleting.</div>
4	Verify the information in the confirmation dialog box, then click OK to delete the router.

Performing Router Management Functions

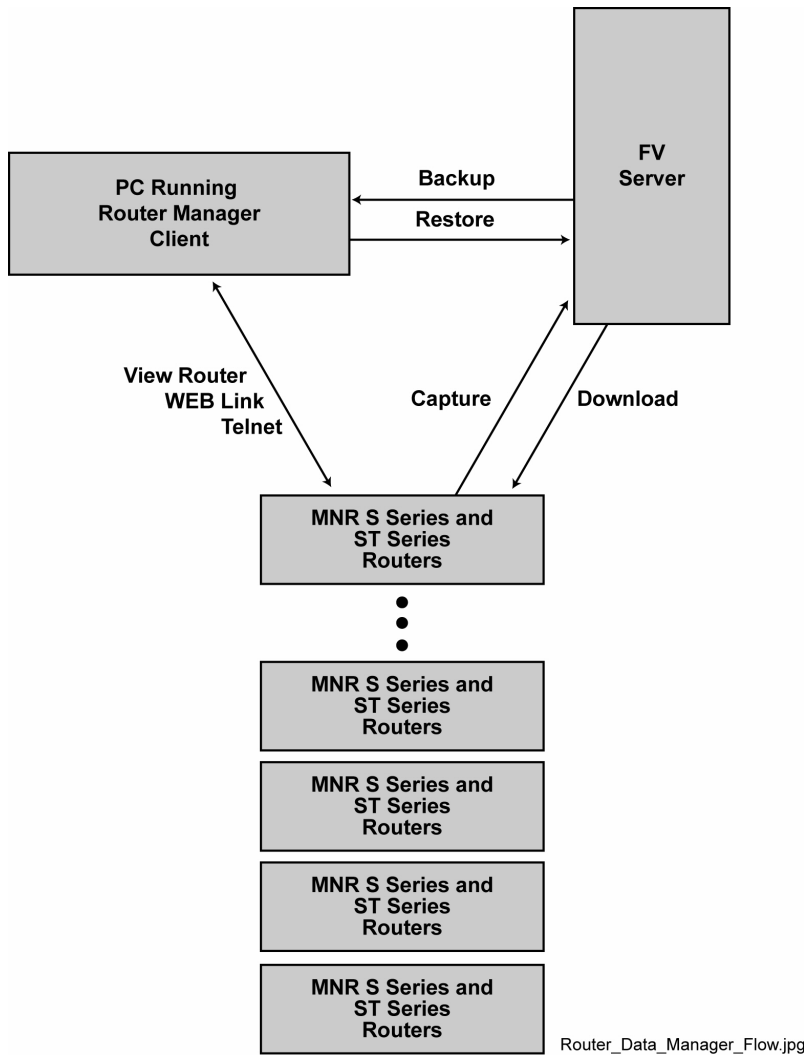
This section describes how to use Router Manager to perform management functions on routers and groups.

Router Manager performs the following functions:

- "Downloading Files to Routers" on page 3-14
- "Capturing (Uploading) Files From Routers" on page 3-16
- "Viewing Runtime Logs" on page 3-18
- "Backing Up Router Manager Data Files on the FullVision INM Server" on page 3-21
- "Restoring Router Manager Data Files to the FullVision INM Server" on page 3-23
- "Rebooting Routers" on page 3-25
- "Setting the Boot Block (Reboot Directory)" on page 3-32
- "Viewing Router Information and Launching Configuration Applications" on page 3-33
- "Performing Checksums" on page 3-37
- "Canceling Router Manager Operations" on page 3-39

Figure 3-9 shows the data flow between the PC running the Router Manager client, the FullVision INM server (shown below as NMS Server), and the routers for key Router Manager functions.

Figure 3-9 Router Manager Data Flow Between PC, FullVision INM Server, and Routers



Downloading Files to Routers

Use the Router Manager Download function to download software, configuration files, and other non-software files from the FullVision INM server to selected routers. Typically, you receive new software on a CD-ROM, so you can perform this procedure independent of the Capture function. For this release, the following files are available for download:

- **EOS SW** — EOS software version files, including the boot.ppc file, and (if available) the router WEBLink files.
- **Configuration File (boot.cfg)** — an ASCII text file that contains CLI configuration commands.
- **Password File (user)** — a binary text file that contains all usernames and passwords for non-root users.

Typical applications of the Download function include:

- Downloading new versions of EOS software to multiple routers at the same time.
- Downloading boot.cfg files to multiple routers, so that all routers can be configured using the ASCII Boot feature. (For details about ASCII Boot, see the “Configuring with ASCII Files” chapter of the **Enterprise OS Software User Guide**.)
- Distributing the same password (user) file across all managed routers. Typically, you edit the usernames and passwords of a given router using the EOS CLI, then upload the edited user file to the FullVision INM server, then download the edited file to multiple routers. (For details, see "Capturing (Uploading) Files From Routers" on page 3-16.)



NOTE

For information about how to update MNR S Series and ST Series routers in the field, see "Upgrading EOS Software on Routers in the Field" on page 3-40.

Procedure 3-5 describes how to download files to a router or group of routers.



NOTE

The software must be forwarded to the server before performing this procedure.

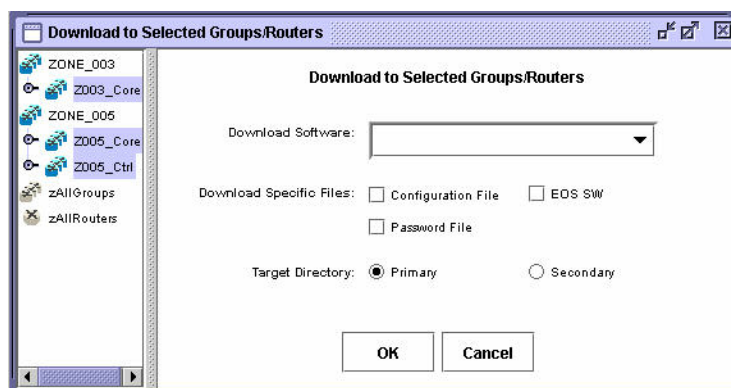
Procedure 3-5 How to Download Files from the FullVision INM Server to Routers

- 1 In the group browser, select the groups or routers to which you want to download files.
- 2 From the Action menu, select **Download** (or click the **Download** toolbar button).




Result: The Download display appears (Figure 3-10).

Figure 3-10 Router Manager Download Display



Procedure 3-5 How to Download Files from the FullVision INM Server to Routers (Continued)

3	<p>Select the files that you want to download in the Download Specific Files area.</p> <div data-bbox="386 331 488 443">  </div> <div data-bbox="513 354 748 405" style="background-color: #00AEEF; color: white; padding: 5px; text-align: center;">NOTE</div> <p>You must select at least one file to download.</p> <ul style="list-style-type: none"> To download all software files for a particular EOS software version: From the Download Software pull-down list, select the software version that you want to download, and under Download Specific Files, select the EOS SW check box. To download non-software files: Under Download Specific Files, select the check boxes corresponding to the files you want to download. <ul style="list-style-type: none"> Select Configuration File to download the corresponding boot.cfg files from the FullVision INM server to the selected groups or routers. Select Password File to download the user file, which contains all usernames and passwords for non-root users.
4	Under Target Directory , select the appropriate radio button to specify whether you want to download the files to the Primary or Secondary source directory on the selected groups or routers.
5	<p>Click OK.</p> <p>Result: A confirmation dialog appears. This dialog box lists the files you have selected for download and the groups/routers you have selected to receive the download.</p>
6	<p>Verify the information in the confirmation dialog box, then click OK to download the files.</p> <p>Result: The Session Log reports that the download was successful and a Download Command Successful dialog box appears.</p>
7	Click OK to dismiss the dialog box.

Capturing (Uploading) Files From Routers

Use the Router Manager Capture function to capture files from a router and upload them to the FullVision INM server. Files uploaded from the router to the FullVision INM server become the master files for the given router.



NOTE

This function is intended primarily for engineers testing router configurations.



NOTE

You cannot upload EOS software versions from a router to the FullVision INM server.


For this release, the following files are available for capture:

- **Configuration File (boot.cfg)** — an ASCII text file that contains the CLI configuration commands for the router.
- **Router Command Log (capture.cfg)** — an ASCII text file that contains the CLI configuration commands the router has processed since bootup.
- **Password File (user)** — a binary text file that contains all usernames and passwords for non-root users. Typically, you would edit the usernames and passwords of a given router using the EOS CLI, then upload the edited user file to the FullVision INM server, then download the edited file to multiple routers (for details, see "Downloading Files to Routers" on page 3-14).

Procedure 3-6 describes how to capture (upload) files from a router or group of routers.

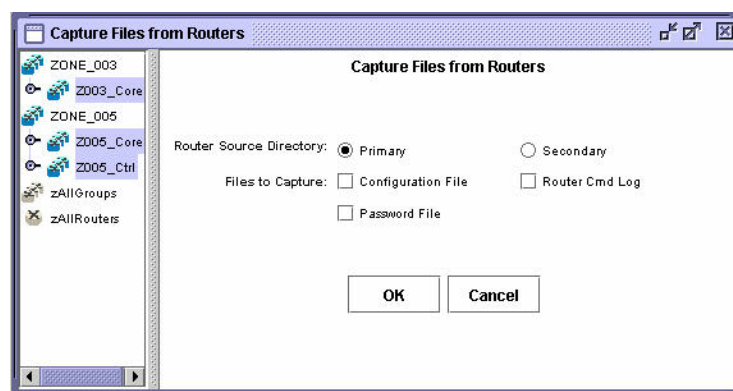
Procedure 3-6 How to Capture (Upload) Files from Routers to the FullVision INM Server

1 In the group browser, select the groups or routers from which you want to upload files.

2 From the Action menu, select **Capture** (or click the **Capture** toolbar button ).


Result: The Capture display appears (Figure 3-11).

Figure 3-11 Router Manager Capture Display



3 Select the appropriate radio button to identify the **Router Source Directory** from which you want to upload files: **Primary** or **Secondary**.

Procedure 3-6 How to Capture (Upload) Files from Routers to the FullVision INM Server (Continued)

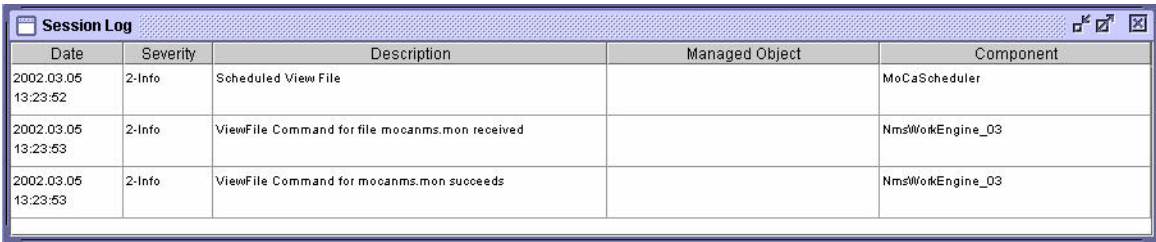
4	<p>Select the check box(es) corresponding to the files you want to upload (Files to Capture):</p> <div data-bbox="386 359 488 470">  </div> <div data-bbox="513 384 748 434"> NOTE </div> <p>You must select at least one file to upload.</p> <ul style="list-style-type: none"> • Configuration File — boot.cfg; an ASCII text file that contains the CLI configuration commands for the router. • Password File — user; a binary text file that contains all usernames and passwords for non-root users. • Router Command Log — capture.cfg; an ASCII text file that contains the CLI configuration commands the router has processed since bootup.
5	<p>Click OK.</p> <p>Result: A confirmation dialog box appears. This dialog box lists the files you have selected for capture and router source directory from which the selected files will be uploaded.</p>
6	<p>Verify the information in the confirmation dialog box, then click OK to upload the files.</p> <p>Result: The Session Log reports that the capture was successful and a Capture Command Successful dialog box appears.</p>
7	<p>Click OK to dismiss the dialog box.</p>

Viewing Runtime Logs

Use the Router Manager Log function to view runtime logs. These are status displays that monitor error and status messages from the FullVision INM server backend. You can view the following types of runtime logs:

- **Session Log** — displays only messages pertaining to commands initiated by the user who is currently logged in to Router Manager. A Session Log opens by default when you log on to Router Manager. As you initiate commands and these commands are executed by the system, status information is displayed in the session log.
- **Full Log** — displays messages pertaining to commands initiated by all users.

Figure 3-12 shows a sample Router Manager session log.

Figure 3-12 Router Manager Session Log


Date	Severity	Description	Managed Object	Component
2002.03.05 13:23:52	2-Info	Scheduled View File		MoCaScheduler
2002.03.05 13:23:53	2-Info	ViewFile Command for file mocanms.mon received		NmsWorkEngine_03
2002.03.05 13:23:53	2-Info	ViewFile Command for mocanms.mon succeeds		NmsWorkEngine_03

As shown in Figure 3-12, the runtime logs are presented as tables, with each row representing a status or error message. The columns of the runtime log tables provide details about the user actions and system responses that generated the messages:

- **Date** — the date and time at which the user action or system response occurred.
- **Severity** — the severity of the user action or system response: **ERROR**, **WARNING**, **INFO**, or **DEBUG**.
- **Description** — a description of the user action or system response.
- **Managed object** (if applicable) — the managed object (router or group) on which the user action was performed.
- **Component** — the FullVision INM server component used to perform the action.
- **Session** (Full Log only) — the username of the user who initiated the action.

By default, Router Manager runtime log tables are sorted by date. You can sort by any of the other columns by clicking the heading of the desired column. In addition, you can resize the columns as necessary to view all the information in a table by clicking and dragging a column boundary in the header row.

Runtime logs continue to fill while you are logged on to Router Manager. When a table includes more rows than can be displayed on a single page, scroll bars appear on the right side of the display to enable you to move through the table.

Viewing the Session Log

To view the Session Log:

From the View menu, select **Session Log** or click the **Session Log** toolbar button .



Viewing the Full Log

To view the Full Log:

From the View menu, select **Full Log** or click the **Full Log** toolbar button .



Viewing Daily Server Log Files

Router Manager stores the server logs in files by day of the week. A specific daily system log displays all historical interactions with the FullVision INM server for all routers. The daily server log files are overwritten the next week.



NOTE

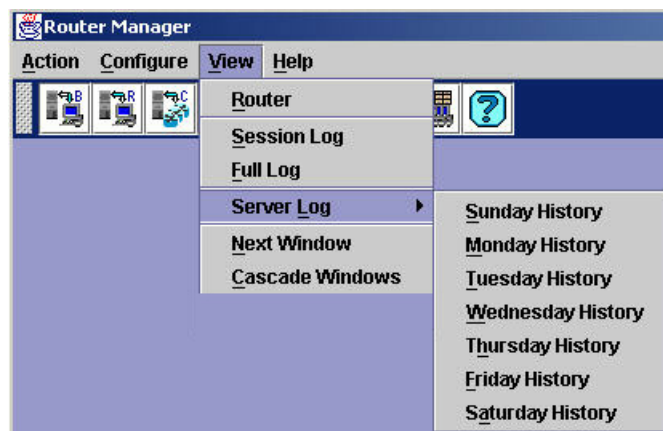
To view daily server logs for a specific router, use the **View Files** option on the View Router display. For details, see "Viewing Router Information and Launching Configuration Applications" on page 3-33.

Procedure 3-7 describes how to view a daily log file.

Procedure 3-7 How to View Daily Server Log Files

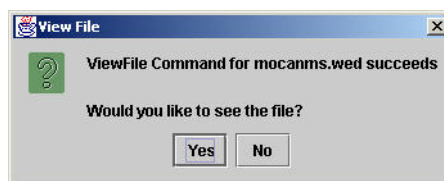
- 1 From the View menu, select **Server Log**.
Result: A submenu of server log file options appear (Figure 3-13).

Figure 3-13 View Server Log Submenu



- 2 Select the option corresponding to the day of the week for which you want to view a server log file: **Sunday History**, **Monday History**, **Tuesday History**, **Wednesday History**, **Thursday History**, **Friday History**, or **Saturday History**.
Result: The View File confirmation dialog box appears (Figure 3-14), asking if you want to view the selected log file.

Figure 3-14 View File Dialog Box



- 3 Click **Yes** to open the selected log file in a browser window.
Result: The browser window for that day appears, showing the server activity.

Backing Up Router Manager Data Files on the FullVision INM Server

Use the Router Manager Backup function to back up files on the FullVision INM server and save them in a specified tar file on your PC. You can perform the following backups:

- **Configuration Files only** — back up only the configuration (boot.cfg) files.
- **Complete Backup** — back up all Router Manager data contained in the directory /usr/MotRm/data.

Procedure 3-8 describes how to back up files on the FullVision INM server.

Procedure 3-8 How to Back Up Router Manager Data Files on the FullVision INM Server

1

From the Action menu, select **Backup** (or click the **Backup** toolbar button).



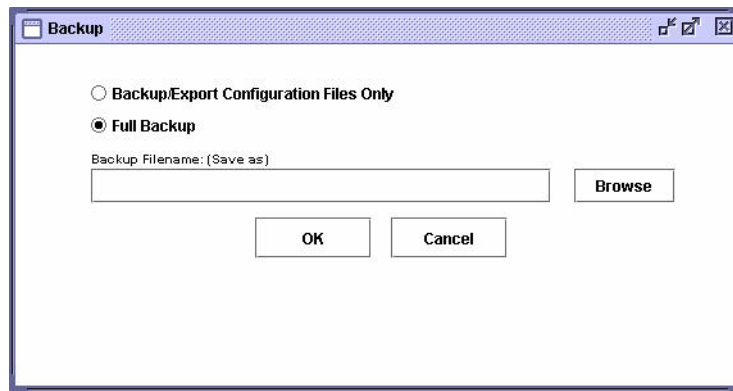
Result: The Backup display appears (Figure 3-15).



NOTE

The Backup function does not back up files directly from the routers; rather, it backs up the router files that are stored on the FullVision INM server.

Figure 3-15 Router Manager Backup Display



2

Specify what files you want to back up by selecting the appropriate radio button.

- Select **Backup/Export Configuration Files Only** to back up router configuration files only.



NOTE

When you use the Router Manager Backup function to back up router configuration files, the boot.cfg update files are encapsulated in a standard UNIX tar-formatted file. This tar file is referred to as the boot.cfg update bundle file (BCUB). For details about the BCUB file, see "BCUB File Format" on page 3-54.

- Select **Full Backup** to back up all Router Manager data.

Procedure 3-8 How to Back Up Router Manager Data Files on the FullVision INM Server (Continued)

3	<p>Specify the file on your PC to which you want to save the backup.</p> <ul style="list-style-type: none"> • If you know the filename and complete path, enter this information in the Backup Filename field. • If you do not know the filename and complete path, click Browse to open a Browse window in which you can browse to the desired directory and enter or select a filename. After you enter or select a filename, click Select to return to the Backup display. This is where the filename and path you specified will now be listed in the Backup Filename field.
4	<p>Click OK.</p> <p>Result: A confirmation dialog box appears. This dialog box indicates whether you have elected to back up only configuration files or to back up all (Router Manager) files on the FullVision INM server. It also lists the file on your PC to which the backup will be saved. The Session Log reports that the backup was successful and a Your Backup Has Completed dialog box appears.</p>
5	<p>Click OK to back up the files from the FullVision INM server to the specified file on your PC.</p>
6	<p>Click OK to dismiss the dialog box.</p>

Restoring Router Manager Data Files to the FullVision INM Server

Use the Router Manager Restore function to input new files or to restore backup files to the FullVision INM server. For this release, you can restore the following:

- Full builds of new EOS software. Full builds are delivered on a CD in a format that is understood by the Router Manager Restore function.
- Engineering builds of new EOS software.
- Backups created by the Router Manager Backup function. (For details about the Backup function, see "Backing Up Router Manager Data Files on the FullVision INM Server" on page 3-21.)



NOTE

You must restore all files in the backup file; partial restores are not supported at this time.

- System configuration updates. These updates should be in boot.cfg update bundle (BCUB) file format. (For details about this file format, see "BCUB File Format" on page 3-54.)

When you restore router files, the restored files become the new master files. When you restore EOS software versions, they overwrite the existing files on the FullVision INM server.


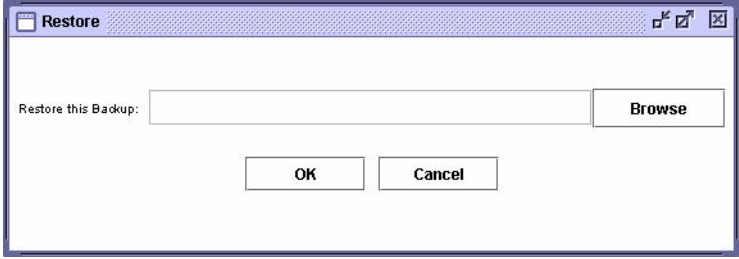


NOTE

The Restore function does not copy files to the routers; rather, it copies files to the FullVision INM server. In order to copy files that you have restored using the Restore function to routers, you must download the files using the Download function. For details, see "Downloading Files to Routers" on page 3-14.

Procedure 3-9 describes how to restore files to the FullVision INM server.

Procedure 3-9 How to Restore Router Manager Data Files to the FullVision INM Server

1	Copy the file you want to restore to an appropriate directory on your PC or insert the CD that contains the files.
2	<p>From the Action menu, select Restore (or click the Restore toolbar button). </p> <p>Result: The Restore display appears (Figure 3-16).</p> <p>Figure 3-16 Router Manager Restore Display</p> 
3	<p>In the Restore this Backup field, specify the file on your PC which you want to restore to the FullVision INM server.</p> <ul style="list-style-type: none"> • If you know the filename and complete path, enter this information in the Restore this Backup field. • If you do not know the filename and complete path, click Browse to open a Browse window in which you can browse to the desired directory and enter or select a filename. After you enter or select a filename, click Select to return to the Restore display. This is where the filename and path you specified will now be listed in the Restore this Backup field.
4	<p>Click OK.</p> <p>Result: A confirmation dialog box appears. This dialog box lists the filename of the file on your PC which will be restored to the FullVision INM server.</p>
5	<p>Verify the information in the confirmation dialog box, then click OK to restore the file to the FullVision INM server.</p> <p>Result: The Session Log reports that the restore was successful and a Restore Has Completed dialog box appears.</p>
6	Click OK to dismiss the dialog box.

Rebooting Routers

Use the Router Manager Reboot function to reboot selected groups and routers; either immediately, in a specified amount of time, or at a specified time.



NOTE

If desired, before you perform the reboot operation you can specify the boot source you want the routers to use. This ensures that if the specified boot source fails, the routers will not reboot from the other boot source. For details see "Setting the Boot Block (Reboot Directory)" on page 3-32.

Performing Immediate Reboots

Procedure 3-10 describes how to perform an immediate router reboot.

Procedure 3-10 How to Perform an Immediate Reboot

1 In the group browser, select the groups or routers you want to reboot.


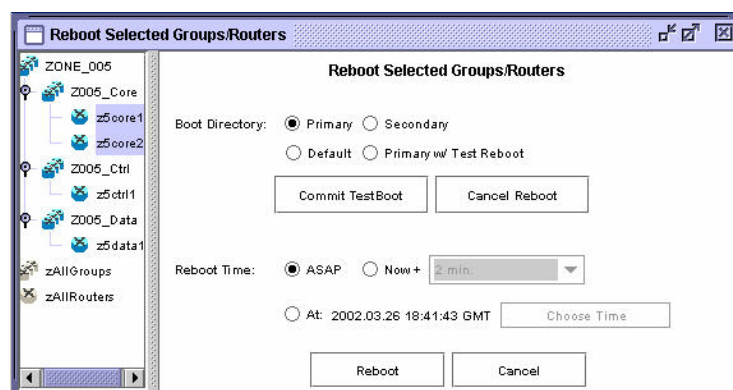
2 From the Action menu, select **Reboot** (or click the **Reboot** toolbar button). 
Result: The Reboot display appears (Figure 3-17).

Figure 3-17 Router Manager Reboot Display



Procedure 3-10 How to Perform an Immediate Reboot (Continued)

3	<p>Specify the Boot Directory.</p> <ul style="list-style-type: none">• If you select the Primary radio button, Router Manager reconfigures the routers to boot from the primary directory prior to the reboot.• If you select the Default radio button, Router Manager does not reconfigure the routers' boot directory prior to the reboot; each router reboots from whatever directory is currently set as the boot directory on that router.• If you select the Secondary radio button, Router Manager reconfigures the routers to boot from the secondary directory prior to the reboot.• If you select the Primary w/Test Reboot radio button, Router Manager reboots the selected routers from the primary boot directory and starts a five-minute watchdog timer. You can then test connectivity with the routers and either cancel the watchdog timer or allow it to expire, in which case Router Manger performs a failover reboot from the secondary directory. This option is particularly useful if your routers are installed at a considerable distance from your location.
4	Under Reboot Time , select the ASAP radio button.

Procedure 3-10 How to Perform an Immediate Reboot (Continued)**5** Click **Reboot**.

Result: A confirmation dialog box appears. This dialog box indicates that the selected routers will be rebooted ASAP, lists the groups and routers which will be rebooted, and specifies the directory from which the routers will be rebooted (*Primary, Secondary, Default, or Primary w/ Test Reboot*).

6 Verify the information in the confirmation dialog box, then click **OK** to reboot the specified routers.**IMPORTANT**

If you selected the **Primary w/Test Reboot** option, Router Manager reboots the selected routers from the primary boot directory and starts a five-minute watchdog timer. As soon as you initiate the reboot (by clicking **OK** from the confirmation dialog box), you should test connectivity with the routers (by pinging them, for example). You then have the following options:

- If your connectivity tests indicate that the reboot was successful and the routers are communicating, click **Commit TestBoot** to cancel the watchdog timer.
- If your connectivity tests indicate that there may be problems with the routers, do not click any button. When the watchdog timer expires, the routers will automatically reboot from the secondary boot directory.

**NOTE**

You cannot use the **Cancel Reboot** button to cancel the failover reboot that occurs when the watchdog timer initiated with the **Primary w/Test Reboot** option expires. The **Cancel Reboot** option cancels only scheduled reboots.

Performing Scheduled Reboots

You can schedule router reboots in either of these ways:

- **Now+** — schedules the reboot to occur in a specified amount of time from the current time. For example schedule the reboot for two hours from now.

- **At** — schedules the reboot to occur at a specific day, hour, minute, and second. For example, schedule the reboot for Tuesday at 11:30:00.



NOTE

Scheduled reboots require EOS software version 11.6 or higher.




NOTE

Router Manager displays reboot times in Greenwich Mean Time (GMT). To ensure that Router Manager calculates the offsets from your time zone correctly, make sure that the system time on your PC, the FullVision INM server, and the routers you are rebooting is set to the correct local time.

Rebooting Routers after a Scheduled Interval

Procedure 3-11 describes how to schedule a router reboot to occur in a specified amount of time from the current time.

Procedure 3-11 How to Schedule a Router Reboot to Occur after a Specified Interval

1	In the group browser, select the groups or routers you want to reboot.
2	From the Action menu, select Reboot (or click the Reboot toolbar button).  Result: The Reboot display appears.
3	Specify the Boot Directory . <ul style="list-style-type: none"> • If you select the Primary radio button, Router Manager reconfigures the routers to boot from the primary directory prior to the reboot. • If you select the Default radio button, Router Manager does not reconfigure the routers' boot directory prior to the reboot; each router reboots from whatever directory is currently set as the boot directory on that router. • If you select the Secondary radio button, Router Manager reconfigures the routers to boot from the secondary directory prior to the reboot.



NOTE

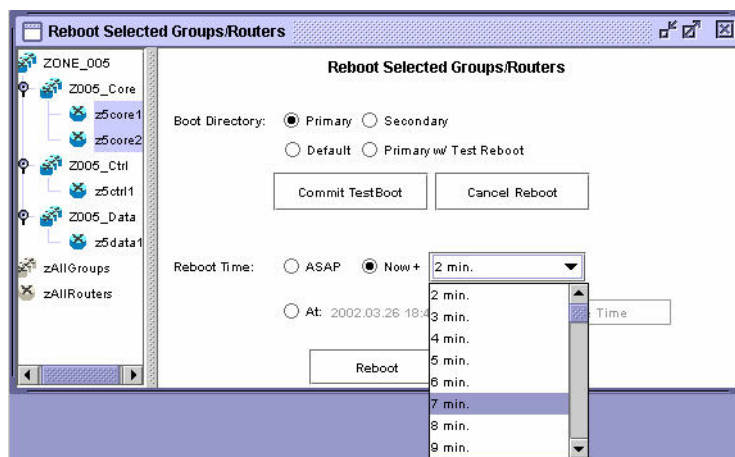
The **Primary w/Test Reboot** option is not available with scheduled reboots.

Procedure 3-11 How to Schedule a Router Reboot to Occur after a Specified Interval (Continued)

- 4** Under **Reboot Time**, select the **Now+** radio button and use the pull-down menu (Figure 3-18) to set the amount of time you want to wait before the reboot.

**NOTE**

The pull-down menu to the right of the **Now+** radio button is activated only when you select the **Now+** radio button on the Reboot display.

Figure 3-18 Router Manager Reboot Now+ Option

- 5** Click **Reboot**.

Result: A confirmation dialog box appears. This dialog box lists the specified reboot time (calculated based on the current time plus the time interval you specified), the groups and routers which will be rebooted, and the directory from which the routers will be rebooted (*Primary*, *Secondary*, or *Default*).

- 6** Verify the information in the confirmation dialog box, then click **OK** to schedule the specified routers to be rebooted at the specified time.

Rebooting Routers at a Scheduled Time

Procedure 3-12 describes how to schedule a router reboot to occur at a specified time.

Procedure 3-12 How to Schedule a Router Reboot to Occur at a Specified Time

- 1** In the group browser, select the groups or routers you want to reboot.

- 2**

From the Action menu, select **Reboot** (or click the **Reboot** toolbar button).



Result: The Reboot display appears.

Procedure 3-12 How to Schedule a Router Reboot to Occur at a Specified Time (Continued)**3** Specify the **Boot Directory**.

- If you select the **Primary** radio button, Router Manager reconfigures the routers to boot from the primary directory prior to the reboot.
- If you select the **Default** radio button, Router Manager does not reconfigure the routers boot directory prior to the reboot; each router reboots from whatever directory is currently set as the boot directory on that router.
- If you select the **Secondary** radio button, Router Manager reconfigures the routers to boot from the secondary directory prior to the reboot.

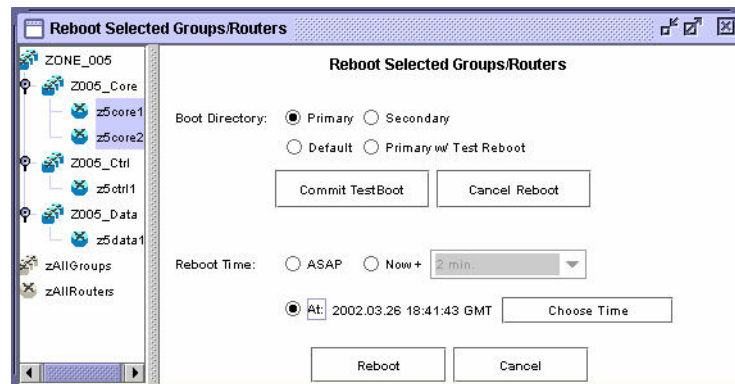
**NOTE**

The **Primary w/Test Reboot** option is not available with scheduled reboots.

4 Select the **At** radio button (Figure 3-19).

Result: The **Choose Time** button is activated.

Figure 3-19 Router Manager Reboot At Option



Procedure 3-12 How to Schedule a Router Reboot to Occur at a Specified Time (Continued)

5 Click **Choose Time**.

Result: The Choose Reboot Time dialog box appears (Figure 3-20).

Figure 3-20 Choose Reboot Time Dialog Box in Router Manager Reboot Window



6 Use the pull-down menus to select the day, hour, minute, and second in GMT at which you want to reboot the routers.

7 Click **OK** to close the Choose Reboot Time dialog box.

8 Click **Reboot**.

Result: A confirmation dialog box appears. This dialog box lists the specified reboot time, the groups and routers which will be rebooted, and the directory from which the routers will be rebooted (*Primary*, *Secondary*, or *Default*).

9 Verify the information in the confirmation dialog box, then click **OK** to schedule the specified routers to be rebooted at the specified time.

Canceling Scheduled Reboots

Procedure 3-13 describes how to cancel a scheduled reboot.

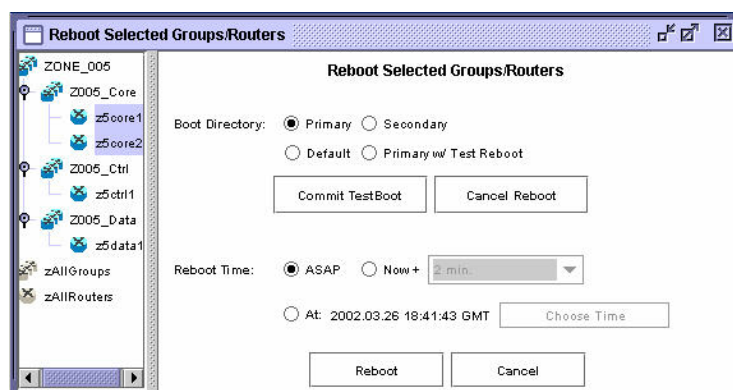
Procedure 3-13 How to Cancel a Scheduled Reboot

1 In the group browser, select the groups or routers for which you want to cancel a scheduled reboot.

2 From the Action menu, select **Reboot** (or click the **Reboot** toolbar button). 

Result: The Reboot display appears (Figure 3-21).

Figure 3-21 Router Manager Reboot Display



3 Click **Cancel Reboot** to cancel any reboots scheduled for the selected routers.



NOTE

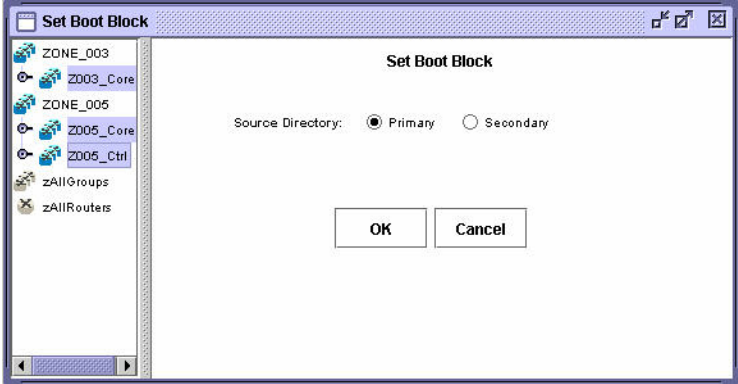
The **Cancel Reboot** option cancels only scheduled reboots; you cannot use it to cancel immediate reboots initiated with **ASAP** selected as the **Reboot Time**.

Setting the Boot Block (Reboot Directory)

Before you reboot a router or group of routers, you can set the boot block. Setting the boot block specifies the boot source you want the routers to use when they reboot (either primary or secondary). The default is primary.

Procedure 3-14 describes how to set the boot block.

Procedure 3-14 How to Set the Boot Block (Reboot Directory)

1	In the group browser, select the groups or routers for which you want to set the boot block.
2	<p>From the Configure menu, select Set Boot Block.</p> <p>Result: The Set Boot Block display appears (Figure 3-22).</p> <p>Figure 3-22 Router Manager Set Boot Block Display</p> 
3	<p>Specify the desired Source Directory by selecting the appropriate radio button.</p> <ul style="list-style-type: none"> • Select Primary to configure the routers to reboot from the primary boot source. • Select Secondary to configure the routers to reboot from the secondary boot source.
4	<p>Click OK.</p> <p>Result: A confirmation dialog box appears. This dialog box lists the groups and routers for which the boot block will be set and boot source to which the boot block will be set (<i>Primary</i> or <i>Secondary</i>).</p>
5	Verify the information in the confirmation dialog box, then click OK to set the reboot directory for the specified routers.

Viewing Router Information and Launching Configuration Applications

Use the Router Manager View Router function to view information about a particular router and to launch configuration applications to be used for a particular router.

From the View Router display, you can do the following:

- View router information, including
 - connection status
 - system name and IP address
 - hardware type
 - date and time of last access and reboot
 - boot directory
 - software version and package loaded in the primary and secondary boot directories
- Delete the router.
- Launch WEBLink (a Web-based configuration and monitoring tool) for the router.
- Launch a Telnet session for the router. From the Telnet session, you can use the EOS CLI to configure and monitor the router.

Table 3-2 lists the information available in the View Router display.

Table 3-2 View Router Display

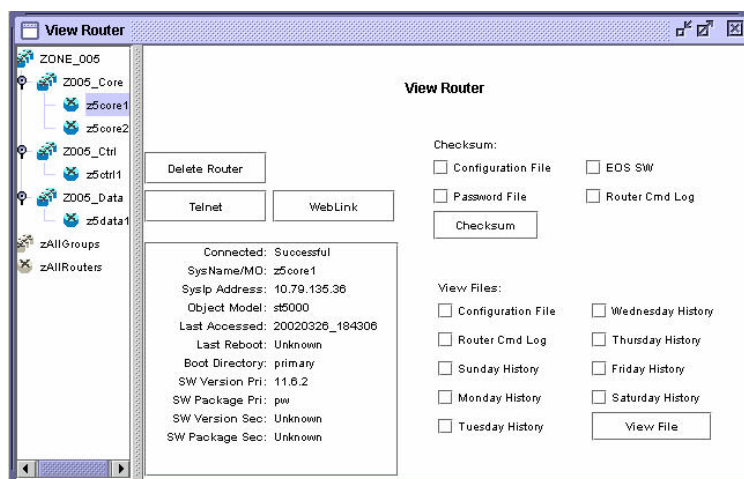
Information in Display	Description
Connected	Connection status of the router.
SysName/MO	System name/managed object name assigned when the router was configured.
SysIP Address	System IP address assigned to the router when it was configured; this is the IP address through which Router Manager communicates with the router.
Object Model	Router hardware type: S4000 or ST5000.
Last Accessed	Date and time at the router was last accessed.
Last Reboot	Date and time at which the router was last rebooted.
Last Boot Directory	Last reboot directory configured for the router.
SW Version Pri	Version of EOS software currently loaded in the router primary boot directory.
SW Package Pri	EOS software package currently loaded in the router primary boot directory.
SW Version Sec	Version of EOS software currently loaded in the router secondary boot directory.
SW Package Sec	EOS software package currently loaded in the router secondary boot directory.

Procedure 3-15 describes how to view router information or launch configuration applications for a particular router.

Procedure 3-15 How to View Router Information and Launch Configuration Applications

- 1** In the group browser, select the router you want to view or edit.
- 2** From the View menu, select **Router**.
Result: The View Router display appears (Figure 3-23). If necessary, click and drag the lower right corner of the window to display all the information.

Figure 3-23 Router Manager View Router Display



NOTE

If Router Manager is able to communicate with the router, an information dialog appears, informing you that the managed object probe was successful. If the managed object probe is not successful, an alert dialog box appears to inform you of this fact. Click **OK** to close the dialog box.

Procedure 3-15 How to View Router Information and Launch Configuration Applications (Continued)

3 Perform the desired operation on the selected router.

- Click **Delete Router** to delete a router. A confirmation dialog box appears. Verify the information in the dialog box, then click **OK** to delete the router. For details about deleting routers, see "Deleting Routers" on page 3-12.
- Click **Telnet** to start a Telnet session for the router.

**NOTE**

The logon for Telnet and WEBLink is confidential and provided by Motorola to approved users. Contact your Motorola support person for more information.

For information about how to use the EOS CLI to configure the router, see the **Enterprise OS Software User Guide** and the **Enterprise OS Software Reference Guide**.

- Click **WebLink** to launch WEBLink against the router. For information about how to use WEBLink, see "Using WEBLink" on page 3-54 or "Using WEBLink" in the "Logging on and Performing Administrative Tasks" chapter of the appropriate hardware user guide.
- Select the check box(es) corresponding to the files on which you want to perform the checksum, then click **Checksum** to perform checksum calculations on router files. A confirmation dialog box appears. Verify the information in the dialog, then click **OK** to initiate the checksum.

**NOTE**

By default, checksums initiated from the View Router display are performed on both the primary and secondary directories and both consistencies and inconsistencies are reported. (For details about performing checksums, see "Performing Checksums" on page 3-37.)

Procedure 3-15 How to View Router Information and Launch Configuration Applications (Continued)

- Select the check box(es) corresponding to the files you want to view, then click **View File** to view **router files**.

You can view the router configuration (boot.cfg) file, the router command log (capture.cfg file), or history files, by day.

**NOTE**

The router history files are similar to the server runtime logs accessed from the **Server Log** option available from the View menu in that they report all historical interaction with the FullVision INM server on a daily basis. However the history files available from the View Router display are specific to the selected router.

- If the view file command is successful, a View File dialog opens. Click **Yes** to view the specified file.
- If the view file command is not successful, an alert dialog box appears, informing you why the command failed.

Performing Checksums

Use the Router Manager Checksum function to perform checksum calculations on one or more routers. These calculations verify the validity of key router files. You can direct Router Manager to check the files on the router against the files stored for the router on the FullVision INM server; any inconsistencies are reported in the runtime log displays.

- To open the Session Log display, from the View menu, select **Session Log**.
- To open the Full Log display, from the View menu, select **Full Log**.

For details, see "Viewing Runtime Logs" on page 3-18.

**NOTE**

You can also perform checksum calculations on an individual router from the View Router display. For details, see "Viewing Router Information and Launching Configuration Applications" on page 3-33.

Procedure 3-16 describes how to perform checksum calculations on one or more routers.


Procedure 3-16 How to Perform Checksum Calculations

- 1 In the group browser, select the groups or routers on which you want to perform checksums.



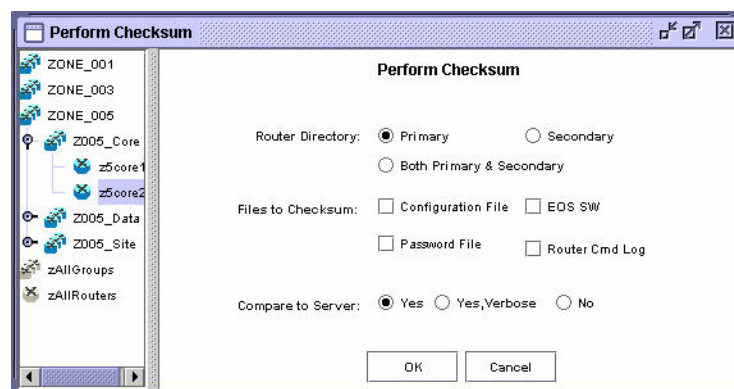
NOTE

If you select a group, Router Manager ungroups it for the purposes of the checksum operation, so that the calculations are performed on each individual router.

- 2 From the Action menu, select **Checksum** (or click the **Checksum** toolbar button ).

Result: The Perform Checksum display appears (Figure 3-24).

Figure 3-24 Router Manager Perform Checksum Display



- 3 Specify the **Router Directory** where you want to perform the checksum:
 - To perform the checksum calculation on files in the router's primary source directory, select the **Primary** radio button.
 - To perform the checksum calculation on files in the router's secondary source directory, select the **Secondary** radio button.
 - To perform the checksum calculation on files in the router's primary **and** secondary source directories, select the **Both Primary & Secondary** radio button.

Procedure 3-16 How to Perform Checksum Calculations (Continued)

4	<p>Specify the Files to Checksum by selecting the appropriate check boxes:</p> <ul style="list-style-type: none"> • Configuration File — Perform a checksum on the boot.cfg files corresponding to the selected routers. The boot.cfg file is an ASCII text file that contains CLI configuration commands. • Password File — Perform a checksum on the password files corresponding to the selected routers. The password file is a binary text file that contains all usernames and passwords for non-root users. • EOS SW — Perform a checksum on the boot.ppc files stored on the selected routers. • Router Cmd Log — Perform a checksum on the capture.cfg files corresponding to the selected routers. The capture.cfg file is an ASCII text file that contains the CLI configuration commands the router has processed since bootup.
5	<p>Indicate whether or not you want Router Manager to compare the checksum calculations to the checksums of the files stored on the FullVision INM server by selecting the appropriate radio button under Compare to Server:</p> <ul style="list-style-type: none"> • Yes — Compare the checksums to those of the files stored on the FullVision INM server and report the inconsistencies only. No reports are written to the log file when the checksums match. • Yes, Verbose — Compare the checksums to those of the files stored on the FullVision INM server and report both the inconsistencies and the consistencies. • No — Do not compare the checksums to those of the files stored on the FullVision INM server.
6	<p>Click OK.</p> <p>Result: A confirmation dialog box appears. This dialog box lists the boot directory in which the checksum will be performed, the files that will be checksummed, and the groups and routers on which checksum will be performed. It also indicates your Compare to Server Settings:</p> <ul style="list-style-type: none"> • Report checksums that differ from server (Yes) • Report all checksums (Yes, Verbose) • Don't compare with server (No)
7	<p>Verify the information in the confirmation dialog box, then click OK to performed the specified checksum calculations.</p> <p>Result: The Session Log reports that the checksum was successful and a Checksum Command Successful dialog box appears.</p>
8	<p>Click OK to dismiss the dialog box.</p>

Canceling Router Manager Operations

You can cancel scheduled Router Manager operations as long as the work engine has not yet begun the job. Jobs are various operations, such as downloads, that involve bigger groups of files.

To determine the status of a job, open a session or full log. (For details, see "Viewing Runtime Logs" on page 3-18.)

Procedure 3-17 describes how to cancel Router Manager operations.

Procedure 3-17 How to Cancel Router Manager Operations

1	<p>Select the appropriate option from the Action menu:</p> <ul style="list-style-type: none">• To cancel all jobs from your session currently queued for the scheduler, select Cancel My Jobs.• To cancel all jobs currently queued for the scheduler, select Cancel All Jobs. <p>Result: A confirmation dialog box appears, asking you to confirm the cancel job request.</p>
2	<p>Click Yes to cancel the jobs.</p>

Upgrading EOS Software on Routers in the Field

This section provides the recommended procedures for performing EOS software upgrades on routers in the field. You must perform these procedures in the order presented.



IMPORTANT

Do not perform this procedure unless Motorola has provided a router software update.



IMPORTANT

If you are upgrading from EOS software version 11.5x or earlier to EOS software version 11.6x or later, you must upgrade the router firmware using the firmware/software portal. For details, see "Using the Portal to Upgrade EOS Firmware with Router Manager" on page 3-45.

**NOTE**


This procedure assumes the following:

- The new EOS code executables are present on the FullVision INM server. (For information about how to update files on the FullVision INM server, see "Restoring Router Manager Data Files to the FullVision INM Server" on page 3-23.)
- The existing EOS software is loaded in both the primary and secondary boot directories on the routers to be upgraded.

Downloading the New EOS Software to the Primary Directory

Procedure 3-18 describes how to download the new EOS software to the primary directory of the selected routers.

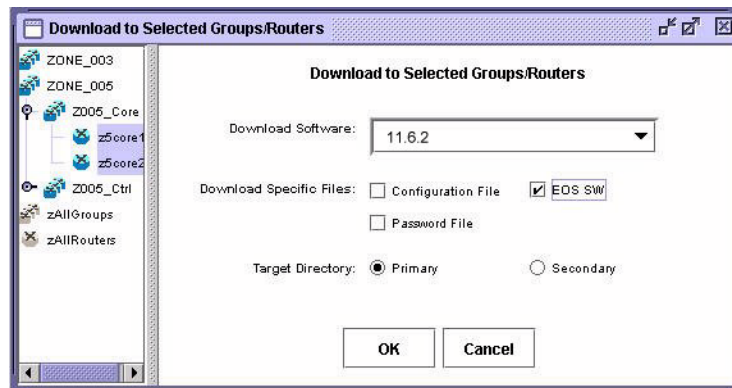
Procedure 3-18 How to Download the New EOS Software to the Primary Directory

1	Forward the software from the client to the server. From the CD that contains the new software, perform "Restoring Router Manager Data Files to the FullVision INM Server" on page 3-23.
2	In the Router Manager window, select the routers you want to update.
3	From the Action menu, select Download (or click the Download toolbar button) to download the new EOS software to the primary directory of the selected routers.  Result: The Download display appears.

Procedure 3-18 How to Download the New EOS Software to the Primary Directory (Continued)

- 4** Make the following selections in the Download display, as shown in Figure 3-25.
 - From the **Download Software** pull-down list, select the software version that you want to download.
 - Under **Download Specific Files**, select the **EOS SW** check box.
 - Under **PrimaryTarget Directory**, select **Primary**.

Figure 3-25 Making Selections on the Router Manager Download Display



- 5** Click **OK**.

Result: A confirmation dialog box appears. This dialog box lists the files you have selected for download, the groups/routers you have selected to receive the download, and the target directory for the download.
- 6** Verify the information in the confirmation dialog box, then click **OK** to download the new software to the primary directory on the selected routers. At this point, the primary directory on the routers selected for update contains the new software version, and the secondary directory contains the old software version.


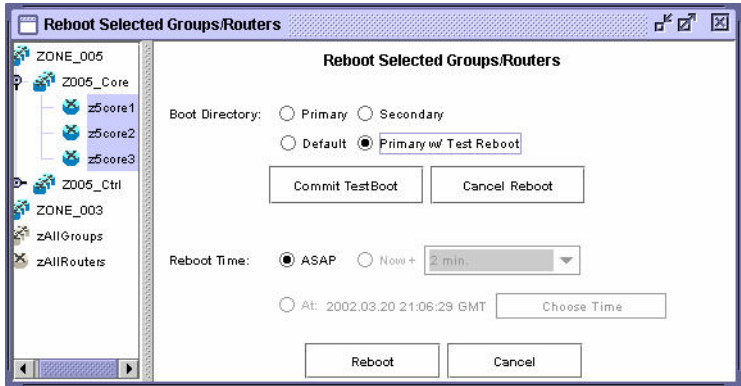
Result: The Download request is sent, and the Session Log reports that the download has started.
- 7** Wait several minutes until the download succeeds.

Result: The Session Log shows that the download was successful and a Download Command Successful dialog box appears.
- 8** Click **OK** to dismiss the dialog box.
- 9** Continue to Procedure 3-19.

Rebooting the Routers and Verifying the Software Upgrade

Procedure 3-19 describes how to reboot the routers and verify the software upgrade.

Procedure 3-19 How to Reboot the Routers and Verify the Software Upgrade

1	<p>From the Action menu, select Reboot (or click the Reboot toolbar button). </p> <p>Result: The Reboot display appears.</p>
2	<p>Make the following selections in the Reboot display, as shown in Figure 3-26:</p> <ul style="list-style-type: none"> Under Boot Directory, select Primary w/Test Reboot. Under Reboot Time, select ASAP.
<p>Figure 3-26 Making Selections on the Router Manager Reboot Display</p> 	
3	<p>Click Reboot to reboot the selected routers.</p> <p>Result: The Session Log shows that the reboot was successful, and a dialog box appears that indicates the command was successful. Click OK to dismiss the dialog box. Since you have selected the Primary w/Test Reboot option, Router Manager sets a five-minute watchdog timer.</p> <ul style="list-style-type: none"> If the routers come up successfully, they will boot from their primary directories running the new software. If the routers do not come up successfully, the watchdog timer will expire and the routers will reboot from their secondary directories running the old software.
4	<p>Wait 1 to 2 minutes.</p>
5	<p>From the View menu, select Router.</p> <p>Result: The View Router display appears. Use this display to verify that the routers came up on the primary directory and that the upgrade was successful. The correct software version must appear.</p>

Procedure 3-19 How to Reboot the Routers and Verify the Software Upgrade (Continued)

6	<p>Return to the Reboot display and click Commit TestBoot to cancel the watchdog timer.</p> <p>Result: A Confirm Reboot Request dialog box appears. Click OK to dismiss it.</p> <div data-bbox="386 405 492 516"> </div> <div data-bbox="516 432 751 483"> <p>IMPORTANT</p> </div> <p>A configured router expects the FullVision INM server to communicate with it shortly after the reboot is complete. If you do not click Commit TestBoot before the watchdog timer expires, the router will reboot from its secondary directory running the old software.</p>
7	<p>Continue to Procedure 3-20.</p>

Downloading the EOS Software to the Secondary Directory



NOTE

These procedures can also be used to downgrade EOS software.

At your administrator's discretion, after the stability of the new software has been evidenced by the system being up and running for an extended period of time, follow these steps to download the new EOS software to the secondary directory of the selected routers:




NOTE

It is recommended that you retain a copy of the old software on the FullVision INM server as a backup so you can downgrade routers in the field to the older software version if necessary.

Procedure 3-20 describes how to download the EOS software to the secondary directory.

Procedure 3-20 How to Download the EOS Software to the Secondary Directory

1	<p>From the Action menu, select Download (or click the Download toolbar button ).</p> <p>Result: The Download display appears.</p>
2	<p>Make the following selections in the Download display:</p> <ul style="list-style-type: none"> From the Download Software pull-down list, select the new EOS software version. Under Download Specific Files, select the EOS SW check box. Under SecondaryTarget Directory, select Secondary.
3	<p>Click OK.</p> <p>Result: A confirmation dialog box appears. This dialog box lists the files you have selected for download, the groups/routers you have selected to receive the download, and the target directory for the download.</p>
4	<p>Verify the information in the confirmation dialog box, then click OK to download the new software to the secondary directory on the selected routers.</p> <p>Result: At this point, the new software version is loaded in both the primary directory and the secondary directory on the selected routers.</p>

Using the Portal to Upgrade EOS Firmware with Router Manager

Before migrating from 11.5x or earlier code to 11.6x code, you must upgrade the EOS router firmware. This section explains why you must upgrade EOS router firmware to migrate to rebranded boot images; provides background information about the firmware/software portal; and describes how to upgrade the firmware in MNR S Series and ST Series routers using the portal with Router Manager.



NOTE

The portal upgrade procedure applies only to MNR S Series and ST Series routers.

The information in this section is as follows:

- "General Procedure for Upgrading Router Firmware Using the Portal with Router Manager" on page 3-46 — provides the basic steps required to upgrade EOS router firmware using the portal with Router Manager.
- "Firmware Upgrade Issues" on page 3-47 — discusses why the firmware upgrade is required.
- "Portal Software Overview" on page 3-48 — provides information about the portal itself.
- "Detailed Procedure for Upgrading Router Firmware Using the Portal with Router Manager" on page 3-49 — provides detailed instructions for upgrading firmware in MNR S Series and ST Series routers using the portal with Router Manager.

**NOTE**

The procedures in this section assume that the new EOS code executables are present on the FullVision INM server. For information about how to update files on the FullVision INM server, see "Restoring Router Manager Data Files to the FullVision INM Server" on page 3-23.

General Procedure for Upgrading Router Firmware Using the Portal with Router Manager

Procedure 3-21 describes the basic steps to allow routers running firmware/software 11.5x or earlier to accept rebranded (11.6x or later) boot images.



NOTE

For more detailed instructions, see "Detailed Procedure for Upgrading Router Firmware Using the Portal with Router Manager" on page 3-49.

Procedure 3-21 How to Upgrade Router Firmware Using the Portal with Router Manager (General Procedure)

1	From the Router Manager View Router display, click Telnet to start a Telnet session for the router.
2	Use the SysconF command (sf) to verify that the router's boot sources are set as follows: <ul style="list-style-type: none"> • Primary boot source = a:/primary/boot.ppc • Secondary boot source = a:/secondar/boot.ppc • Boot sources = primary and secondary • Test boot source = a:/primary/boot.ppc
3	From the Router Manager Download display, download the portal boot image (11.5.22I) to the routers' secondary boot directory.
4	From the Router Manager Download display, download the rebranded boot image to the routers' primary boot directory.
5	From the Router Manager Reboot display, reboot the routers. The primary boot source will show fail, but the router is configured to boot from the secondary boot source if the primary boot source fails. As such, the router boots the portal and the following occurs: <ul style="list-style-type: none"> • The portal detects a firmware mismatch and updates one of the Boot2 boot banks with the portal firmware and makes this boot bank the designated Boot2 boot bank. • The system automatically resets and loads the primary (rebranded) boot image. • Since the portal firmware is now the designated Boot2 boot bank, it boots the rebranded boot image.

Firmware Upgrade Issues

The firmware on MNR S Series and ST Series routers uses two Boot2 boot banks: BOOT2A and BOOT2B. The active Boot2 bank is the "designated" Boot2 bank. The other bank is the "non-designated" Boot2 bank. When you download a new boot image to a router, the firmware does the following:

- Detects the firmware version string mismatch.
- Updates the Boot2 image into the non-designated Boot2 bank.
- If the update is OK and the checksum is good, sets the switch_boot_bank flag, causing the non-designated Boot2 bank to become the designated Boot2 bank.

Firmware updates occur only when a version string mismatch is detected. The firmware version strings are compared to determine if a mismatch is present. These strings include two sub-strings:

- Platform mnemonic string
- Version number string

Normally, the firmware version number sub-string is changed with every new build of firmware. As part of the effort to rebrand the routers, the platform mnemonic sub-string was also changed. S4000/ST5000 firmware recognizes the platform mnemonics and their rebranded counterparts.

You must upgrade the firmware using the firmware/software portal if a router rejects all other boot images, typically returning a boot message similar to:

The image does not appear to be a PB500 image. Load aborted.

Upgrading the firmware allows the router firmware/software to accept rebranded boot images.

Portal Software Overview

The firmware/software portal is a special transitional version of firmware/software. It allows S Series S4000 and ST5000 Series routers running an older firmware/software version to accept rebranded (ST) images.

Table 3-3 summarizes the differences between the PathBuilder, portal, and rebranded (ST) firmware in terms of the following:

- **Platforms recognized**
- **Version strings** contained in the images
- State (OLD or NEW) of the **platform mnemonic** in the version string in the firmware/software product.definition files
- State (OLD or NEW) of the **firmware** in the firmware/software product.definition files

Table 3-3 Comparison of PathBuilder, Portal, and Rebranded (ST) Firmware

FW/SW Version	Platforms Recognized	Version Strings	Platform Mnemonic	Firmware
PathBuilder	PBS400, NBPB500	FW/PBS400-BOOT2,x.y.zzI FW/NBPB500-BOOT2,x.z.zzI	OLD	OLD
Portal	PBS400, NBPB500, S4000, ST5000	FW/PBS400-BOOT2,x.y.zzT FW/NBPB500-BOOT2,x.z.zzT	OLD	NEW
ST (rebranded)	PBS400, NBPB500, S4000, ST5000	FW/ST4000-BOOT2,x.y.zzI FW/ST5000-BOOT2,x.z.zzI	NEW	NEW

The portal is useful when you are downloading and running both the PathBuilder and the rebranded versions of the firmware serially on the same EOS router. If you never move forward to the rebranded firmware, you do not need the portal. If you have migrated to the rebranded firmware and never regress to the old firmware, you no longer need the portal.

Detailed Procedure for Upgrading Router Firmware Using the Portal with Router Manager

This section provides detailed procedures for using the portal with Router Manager to upgrade the EOS firmware on the MNR S Series and ST Series routers so that the routers will accept rebranded boot images. You must perform these procedures in the order presented.

Verifying the Boot Source of the Router

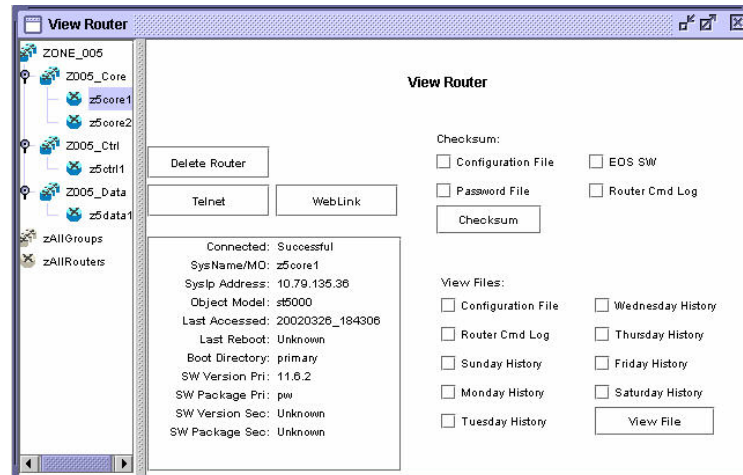
Procedure 3-22 describes how to view the boot source of the router.

Procedure 3-22 How to Verify the Boot Source of the Router

- 1 From the View menu, select **Router**.

Result: The View Router display appears (Figure 3-27).

Figure 3-27 Router Manager View Router Display


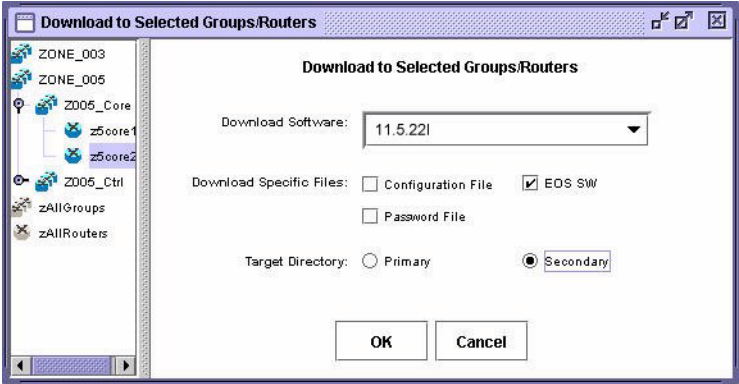


- 2 Click **Telnet** to start a Telnet session for the router.
- 3 Log on as **root** or **admin** with the Network Manager password.
For details about the router root/admin password, see the “Logging on and Performing Administrative Tasks” chapter of the appropriate hardware user guide.
- 4 Use the **SysconF** command (sf) menus to verify that the router’s boot sources are set as follows:
 - Primary boot source = a:/primary/boot.ppc
 - Secondary boot source = a:/secondar/boot.ppc
 - Boot sources = primary and secondary
 - Test boot source = a:/primary/boot.ppc
 For details about the **SysconF** command menus, see the “SysconF Command Menus” appendix in the appropriate hardware user guide.
- 5 Continue to Procedure 3-23.

Downloading the Portal Boot Image to the Secondary Boot Directory

Procedure 3-23 describes how to download the portal boot image (11.5.22I) to the routers' *secondary* boot directory.

Procedure 3-23 How to Download the Portal Boot Image to the Secondary Boot Directory

1	In the group browser, select the groups or routers to which you want to download the portal boot image.
2	<p>From the Action menu, select Download (or click the Download toolbar button ).</p> <p>Result: The Download display appears.</p>
3	<p>In the Download display, make the following selections to configure the portal software to be downloaded to the secondary directory, as shown in Figure 3-28.</p> <ul style="list-style-type: none"> From the Download Software pull-down list, select the portal software (11.5.22I). Under Download Specific Files, select the EOS SW check box. Under Target Directory, select the Secondary radio button. <p>Figure 3-28 Configuring the Portal Software Download</p> 
4	<p>Click OK.</p> <p>Result: A confirmation dialog box appears. This dialog box lists the files you have selected for download, the groups/routers you have selected to receive the download, and the target directory for the download.</p>
5	Verify the information in the confirmation dialog box, then click OK to download the portal software to the routers' secondary boot directory.
6	Back up your current working boot.ppc file.
7	Continue to Procedure 3-24.

Downloading the New Boot Image to the Primary Boot Directory

Procedure 3-24 describes how to download the new boot image to the routers' primary boot directory.

Procedure 3-24 How to Download the New Boot Image to the Primary Boot Directory


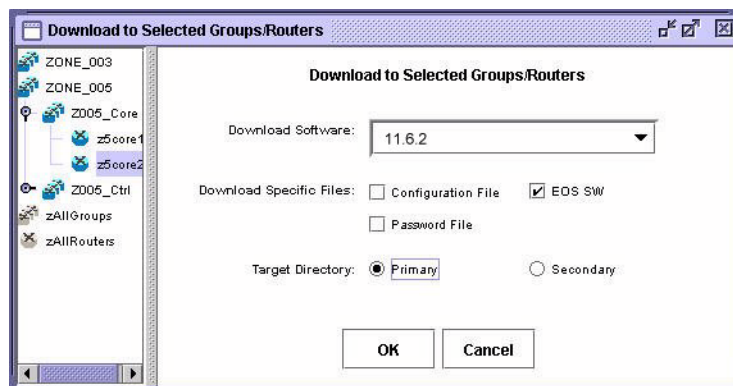
1	In the group browser, select the groups or routers to which you want to download the new boot image.
2	<p>From the Action menu, select Download (or click the Download toolbar button ).</p> <p>Result: The Download display appears.</p>
3	<p>In the Download display, make the following selections to configure the new software to be downloaded to the primary directory, as shown in Figure 3-29.</p> <ul style="list-style-type: none"> From the Download Software pull-down list, select the new software version. Under Download Specific Files, select the EOS SW check box. Under Target Directory, select the Primary radio button.
4	<p>Click OK.</p> <p>Result: A confirmation dialog box appears. This dialog box lists the files you have selected for download, the groups/routers you have selected to receive the download, and the target directory for the download.</p>
5	Verify the information in the confirmation dialog box, then click OK to download the new software to the routers' primary boot directory.
6	Continue to Procedure 3-25.


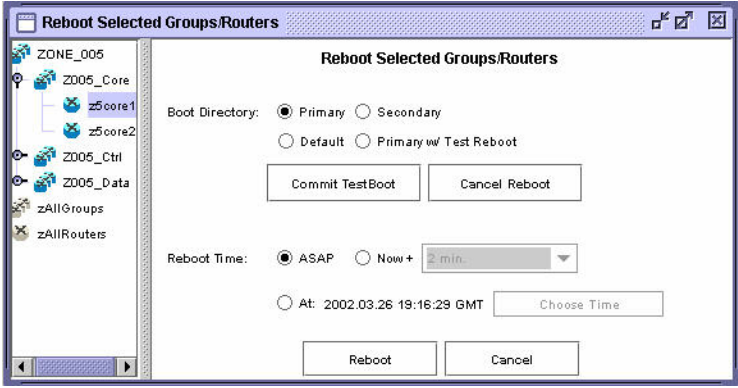
Figure 3-29 Configuring the New Boot Image Download



Rebooting the Routers with the Rebranded Boot Image

Procedure 3-25 describes how to reboot the routers with the rebranded boot image.

Procedure 3-25 How to Reboot the Routers with the Rebranded Boot Image

1	In the group browser, select the groups or routers you want to reboot.
2	<p>From the Action menu, select Reboot (or click the Reboot toolbar button). </p> <p>Result: The Reboot display appears (Figure 3-30).</p> <p>Figure 3-30 Router Manager Reboot Display</p> 
3	Under Boot Directory , select the Primary radio button.
4	Under Reboot Time , select the ASAP radio button.
5	<p>Click Reboot.</p> <p>Result: A confirmation dialog box appears. This dialog box indicates that the selected router will be rebooted ASAP, lists the routers which will be rebooted and specifies the directory from which the router will be rebooted (<i>Primary</i>, <i>Secondary</i>, <i>Default</i>, or <i>Primary w/ Test Reboot</i>).</p>
6	<p>Verify the information in the confirmation dialog box, then click OK to reboot the routers. The primary boot source will show fail, but the router is configured to boot from the secondary boot source if the primary boot source fails. As such, the router boots the portal and the following occurs:</p> <ul style="list-style-type: none"> • The portal detects a firmware mismatch and updates one of the Boot2 boot banks with the portal firmware and makes this boot bank the designated Boot2 boot bank. • The system automatically resets and loads the primary (rebranded) boot image. • Since the portal firmware is now the designated Boot2 boot bank, it boots the rebranded boot image.

BCUB File Format

When you use the Router Manager Backup function to back up router configuration files, the boot.cfg update files are encapsulated in a standard UNIX tar-formatted file. This tar file is referred to as the boot.cfg update bundle (BCUB) file. The format of the BCUB file is as follows:

- The BCUB contains only relative pathnames. Absolute files are not used or contained within the BCUB file.
- No directory structure is contained within the BCUB file. All files in the BCUB file exist at the same directory level.
- The SysName of each router's configuration file is determined per the following specification: *The System Configuration (IP and DSN) Plan*, Revision 1.6, August 13, 2001 Sections 6.4 and 6.5 give examples of the naming convention used.
- The name of each router's configuration file located within the BCUB file is as follows: SysName_SysIPAddress.cfg
For example: z1core1_10.1.1.123.cfg
z2core2_10.2.1.124.cfg z3mgeg3_10.3.1.125.cfg
The SysName specified in this naming convention is the address the FullVision INM server should use to access and control the router.
- The BCUB file contains a text file name MoCaImportBootConfigs. This file may contain UNIX formatted ASCII text describing the information being loaded. The filename triggers the FullVision INM server back end, indicating that the file is indeed a BCUB file.
- The contents of each router's boot.cfg file is contained within each routers SysName_SysIPAddress.cfg file.

Using WEBLink

Router Manager provides a launch point for WEBLink, a graphical user interface (GUI) that enables you to manage MNR S Series and ST Series routers via a Web-based server embedded on the routers. When you use WEBLink, user management is handled by the router itself.

With a few exceptions, WEBLink allows you to execute all the configuration commands available from the router's Telnet command line interface (CLI). The major difference is the user interface: WEBLink is a GUI that offers a more user-friendly configuration method with online help and example commands.

In addition to configuration management options, WEBLink provides performance management in the form of traffic and line error analysis, CPU utilization, and buffer usage information. WEBLink displays this information in historical and real-time graphs and provides details in tables.

**NOTE**

Configuration changes made through WEBLink are temporary and are eliminated when the router is rebooted. Configuration changes made through the CLI, on the other hand, are permanent. To make permanent configuration changes, contact your Motorola service representative.

**NOTE**

You can also access the online help from the WEBLink interface for complete help on individual windows or dialog boxes. For more detailed instructions for using WEBLink, see the appropriate router hardware user guide.

Key Differences Between WEBLink and Router Manager

WEBLink is a GUI for an embedded Web-based server running on the router itself. It provides a more user-friendly way to execute the configuration commands available in the router's CLI, but configuration changes made via WEBLink are not permanent. WEBLink also provides router performance statistics in the form of graphs.

Router Manager is a device management and grouping application that runs on the Full Vision Integrated Network Manager (INM) server. You can use Router Manager to perform a variety of management functions and to back up and restore router files to and from the INM server. You can also use Router Manager to launch WEBLink against a selected Router. In addition, Router Manager integrates fault management for MNR S Series and ST Series routers in HP OpenView.

Launching WEBLink

Procedure 3-26 describes how to launch WEBLink.

Procedure 3-26 How to Launch WEBLink

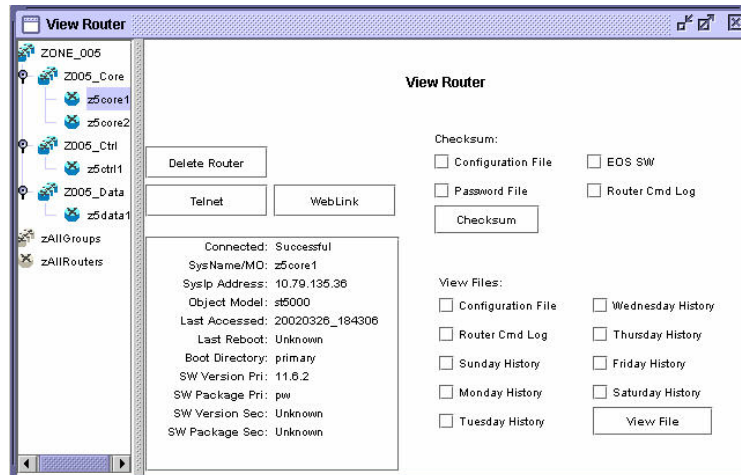
1	In the Router Manager group browser, select a router icon. Result: The device icon is highlighted.
2	From the View menu, select Router to open the View Router display. Result: If Router Manager is able to communicate with the router, an information dialog appears, informing you that the managed object probe was successful. If the managed object probe is not successful, an alert dialog box appears to inform you of this fact. Click OK to dismiss the dialog box.

Procedure 3-26 How to Launch WEBLink (Continued)

3 If necessary, click and drag the lower right corner to display all the information.

Result: The View Router display appears (Figure 3-31).

Figure 3-31 View Router Display



4 To launch WEBLink against the router, click **WebLink**.

Result: The Network Password dialog box appears.

Procedure 3-26 How to Launch WEBLink (Continued)

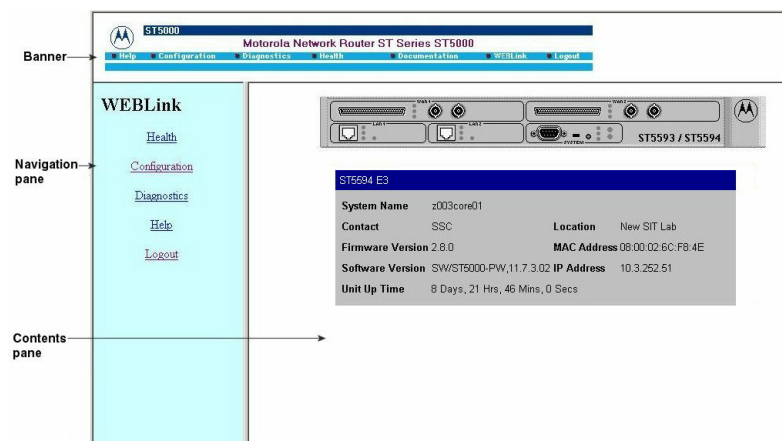
5 In the User Name box, type the logon to access WEBLink, and then press **Enter**.

**NOTE**

The logon is confidential and provided by Motorola to approved users. Contact your Motorola support person for more information.

Result: The WEBLink Web page launches (Figure 3-32).

Figure 3-32 WEBLink Main Interface Window



6 Click a link from the banner or a navigation link to move to one of the following management areas:

- **Health** — provides summary information regarding the health of the device. Available statistics include an overall health summary, interface and protocol performance, as well as Virtual Private Network (VPN) performance.
- **Configuration** — provides the path to display all non-default parameters configured on the routers.
- **Diagnostics** — provides troubleshooting information that may help if you are encountering problems during installation or regular device maintenance. Diagnostic information is available for scanning the internal resources of the device (for example, memory fragmentation, memory usage, system messages, and the local audit log) or regarding specific protocols.
- **Help** — provides online help on how to use the features of the WEBLink interface. Context-sensitive help about every available device parameter or command is also provided on the configuration pages for the specific parameters.
- **Logout** — terminates the http session between the browser client and the router.
- **Documentation** — provides links to access EOS software and hardware documentation.



NOTE

Click the **Help** icon in the navigation pane to access the on-line help, or click the Documentation link for **EOS** router documentation.

Viewing Performance Reports

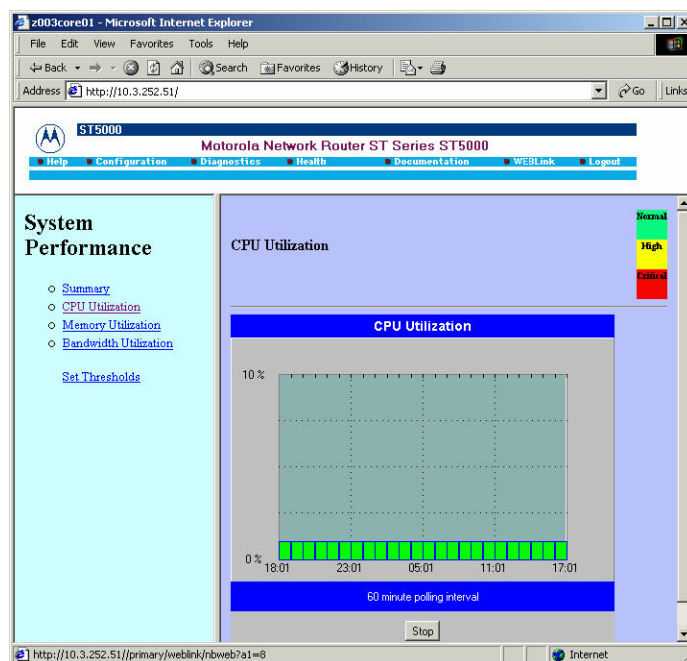
Available statistics include an overall health summary, interface performance, and protocol performance. These statistical graphs help monitor resource usage to aid in troubleshooting problems, assist with capacity planning, and provide data for analysis. The graphs provide historical and real-time data.

Procedure 3-27 describes how to view a performance report from WEBLink.

Procedure 3-27 How to View a Performance Report

- 1 On the WEBLink main window, click the **Health** icon to view summary information regarding the health of a device.
Result: The Health menu appears in the navigation pane.
- 2 Select the desired option. The example below shows the **System Performance** option.
Result: The performance report graph appears (Figure 3-33).

Figure 3-33 Performance Report Graph



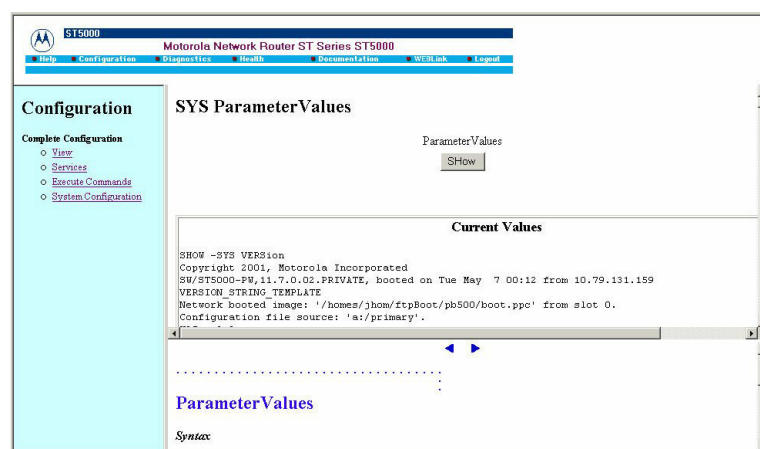
Viewing Router Configuration

Procedure 3-28 describes how to view the router configuration. This configuration summary displays all non-default system parameters currently configured on the Enterprise OS device.

Procedure 3-28 How to View the Router Configuration

- 1** On the WEBLink main window, click the **Configuration** icon.
Result: The Configuration menu options appear in the navigation pane.
- 2** Under Complete Configuration, click **View**.
Result: The router configuration parameters appear (Figure 3-34).

Figure 3-34 Router Configuration Parameters



This page intentionally left blank.

Managing the Remote Terminal Server

The remote terminal server is the access point for all administration with the network management servers, zone controllers, and other IP devices in the zone. Your ASTRO 25 system may include two types of terminal servers: iTouch® or Xyplex®.



NOTE

An ASTRO 25 SE system does not use the Xyplex terminal server. Ignore all references to the Xyplex.



NOTE

An ASTRO 25 SE system does not contain the Cisco Catalyst 6509 Ethernet LAN switch (LAN switch) or Nortel® Passport 7480 WAN switch (WAN switch). Ignore all references to these switches.



NOTE

An ASTRO 25 SE system does not contain the following servers: Transport Network Performance Server (TNPS), Ethernet Switch Management Server (ESMS), and the WAN Switch Management Server (WSMS). Ignore all references to these servers.

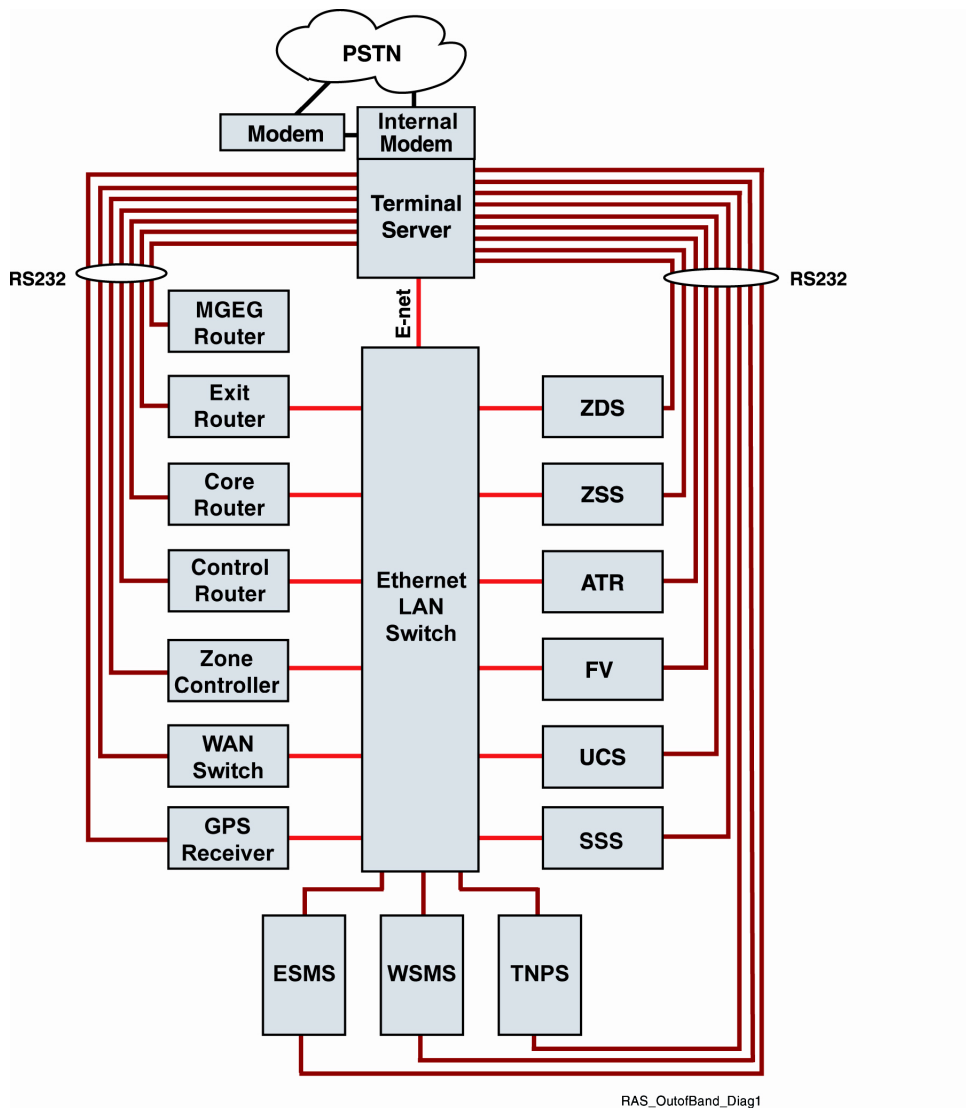
The terminal server should be used when performing any of the administration functions described in Volume 3, *Administering Servers and Controllers*.

This chapter includes the following topics:

- "Diagram of Typical Connections to the Remote Terminal Server" on page 4-2
- "Reasons for Using the Remote Terminal Server" on page 4-3
- "Process for Using the Remote Terminal Server" on page 4-4
- "Remote Terminal Server Command Keys" on page 4-5
- "Logging On to the Remote Terminal Server" on page 4-6
- "Using the Remote Terminal Server to Access a Device" on page 4-10
- "Opening Sessions with a Number of Devices" on page 4-12
- "Opening a Telnet Session with a Host" on page 4-13
- "Resuming a Session with a Device" on page 4-14

- ## Diagram of Typical Connections to the Remote Terminal Server

4-2

Figure 4-1 Remote Terminal Server Connections

Reasons for Using the Remote Terminal Server

The remote terminal server includes a number of benefits that are not available through a direct Telnet connection to a device, such as the following:

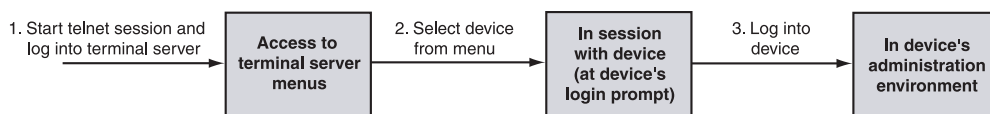
- If you establish a Telnet session directly with a device and fail to log out of the device, you can be locked out of the device, and may need to reset the device or call Motorola® for support.

- A terminal server session can time out, while a direct Telnet session with a device does not time out. Timing out of a session prevents unauthorized access to your devices.
- If you are running Telnet sessions directly to a device, a trail of the individual connections can later be viewed in the Telnet program or the Run command box in Windows®. Using the terminal server prevents individual connection information (other than the terminal server itself) from being exposed to other people accessing the client.

Process for Using the Remote Terminal Server

When administering a device, you must first connect with the terminal server, then select the device from the terminal server menus to establish a session with the device, and finally log onto the administration menu of the individual device to administer it. Figure 4-2 shows the three-step process for accessing a device.

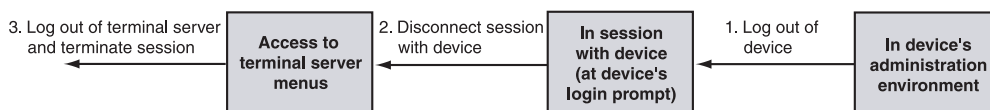
Figure 4-2 Accessing a Device Through the Terminal Server



After administering a device, you must first log out of the device's administration menu, then disconnect the session with the device.

To exit the terminal server, you must log out of all device administration environments and disconnect all device sessions. Then you can log out and disconnect your Telnet session with the terminal server. Figure 4-3 shows the process for disconnecting devices and logging out of the terminal server.

Figure 4-3 Disconnecting Devices and Logging Out of the Remote Terminal Server



Remote Terminal Server Command Keys

Table 4-1 lists command keys that are used to navigate through the terminal server menus or perform different functions. Several of these commands are used in other terminal server procedures in this chapter.





NOTE

Once you have accessed a menu or submenu, the available options appear underneath the menu.

Table 4-1 Remote Terminal Server Commands


Command	Description	When Available
Ctrl+L	Returns to the terminal server menu system.	This command can be used when in a device session or when running system maintenance.
<div><div></div><div>NOTE</div><div>The session with the device remains connected, but the screen reverts to the main menu or appropriate submenu on the terminal server.</div></div>		
Ctrl+K	Switches between open device sessions.	This command can be used at any time (either within the terminal server menu system or in a session with another device).
Ctrl+J	Resumes the previous console port session when one or more sessions have been established.	<div><div></div><div>NOTE</div><div>Device console ports do not support multiple sessions. If you established multiple sessions and are not using all of them, disconnect all sessions, then re-establish the necessary sessions needed. This allows others to access the devices.</div></div>
Shift+Q	Logs out and terminates the session with the terminal server.	<div><div></div><div>NOTE</div><div>This command can only be used in the iTouch terminal server nested menu configuration.</div></div>

Table 4-1 Remote Terminal Server Commands (Continued)

Command	Description	When Available
Shift+R	Refreshes the screen.	<div><div>NOTE</div><p>This command can only be used in the iTouch terminal server nested menu configuration.</p></div>
Shift+T	Displays the main menu of the terminal server.	<div><div>NOTE</div><p>This command can only be used in the iTouch terminal server nested menu configuration.</p></div>
<p>For systems using two 20-port Xyplex terminal servers, use the following control sequences when logged into the second terminal server:</p> <ul style="list-style-type: none">• CTRL+P: Local Switch• CTRL+O: Forward Switch• CTRL+I: Backward Switch		

Logging On to the Remote Terminal Server

This section describes how to access the terminal server.



NOTE

The logon is **motorola**. The password is confidential and provided by Motorola to approved users. Contact your Motorola support person for more information.

Dialing In to the Terminal Server

Follow Procedure 4-1 to dial in to the terminal server with a laptop computer and modem. Use HyperTerminal or ProComm (VT100 emulation).

Procedure 4-1 How to Access the Terminal Server through Dial In

1	Dial the telephone number of the line connected to the modem at the terminal server. Result: The <code>LOGIN></code> prompt appears.
2	Enter the password that you were assigned during configuration. Result: You are prompted to press Enter four times to access interactive mode.
3	Press Enter four times to access the interactive mode. Result: The Welcome screen and the iTouch menu appear.

Accessing the Terminal Server Through Telnet

Procedure 4-2 describes how you can log on to the terminal server. Up to eight terminal server Telnet sessions are available. Additional instructions for selecting devices in the terminal server are provided in Procedure 4-3, "How to Access a Device through the Remote Terminal Server," on page 4-9.

Procedure 4-2 How to Log On to the Remote Terminal Server

1 Initiate a Telnet session with the terminal server.

1. Click the **Start** button on the Windows taskbar.
2. Select **Run...** from the menu.
3. Type **cmd** and press **Enter**.

Result: The cmd.exe window appears. This window hides the IP address that you enter in the next step, for system security.

4. Type **telnet xxx.xxx.xxx.xxx** at the cmd prompt, where **xxx.xxx.xxx.xxx** is the IP address of the terminal server. The IP address varies according to your system ID and zone ID.

5. Press **Enter**.

Result: A window opens with a blank screen.



NOTE

A Telnet session can also be started by using a Telnet application, or can be started by using HyperTerminal or ProComm set with a TCP/IP connection to the terminal server.

2 Press **Enter** until the login prompt appears.



NOTE

The login prompt appears after approximately three tries. Do not press **Enter** multiple times or you will be logged out automatically.

Result: The **LOGIN>** prompt appears.

Procedure 4-2 How to Log On to the Remote Terminal Server (Continued)**3**

At the login prompt, type **motorola** then press **Enter**.

**NOTE**

Your login information is not displayed on the screen while you type.

Result: A welcome message is displayed along with the following prompt:
Enter username>

4

At the prompt, type in a user name to identify your session with the terminal server, such as **user1**, then press **Enter**.

Result: The main menu appears, similar to the screen shown below.
Menu 1: Main Menu

-
1. Maintenance Access
 2. Router Menu
 3. LAN/WAN Switches Menu
 4. ZC/Unix Servers Menu
 5. Other Devices Menu
 6. Telnet Session to Host
 7. Resume a Session
 8. Disconnect a Session
 9. Show Users
-

Logout Q Refresh Screen R
Enter number of selection or use arrow keys:

**NOTE**

This menu may vary slightly depending on your system's configuration.

Using the Remote Terminal Server to Access a Device



After you have logged on to the terminal server and have reached the main menu, you can use Procedure 4-3 to access devices in the zone.

Procedure 4-3 How to Access a Device through the Remote Terminal Server

1

At the main menu of the terminal server, select the device category that you are trying to access.

Result: The submenu for that category is displayed showing a list of devices. An example submenu is shown below.

Menu 4: ZC/Unix Servers

1. Zone Controller 1

2. Zone Controller 2

3. Zone Manager Database Server

4. Zone Statistical Server

5. Air Traffic Router

6. FullVision Server

7. User Configuration Subsystem

8. System Statistical Server

9. WAN Switch MGMT Server

10. Ethernet Switch MGMT Server

Logout Q Refresh Screen R Top Menu T

Enter number of selection or use arrow keys:

NOTE

Your submenu items may be different depending on your particular configuration.

2





At the submenu prompt, select the appropriate device from the list.

Result: A connection is established with the selected device.

NOTE

Devices can only accept one session at a time. Other users will not be able to access the device until your session is closed.



Procedure 4-3 How to Access a Device through the Remote Terminal Server (Continued)

- | | |
|----------|---|
| 3 | <p>Log on and administer the device according to the instructions for the device.</p> <div data-bbox="488 331 586 436"></div> <div data-bbox="612 354 846 405">NOTE</div> <p>If a <root> # prompt appears, type exit to return to the proper prompt.</p> <div data-bbox="488 495 586 600"></div> <div data-bbox="612 518 846 569">NOTE</div> <p>See Volume 3, <i>Administering Servers and Controllers</i> for information about logging in and administering servers and for information about the zone controller.</p> <p>For information about logging in and administering network equipment (such as switches), see Chapter 5, "Managing Other Transport Equipment." For other devices, see the appropriate device documentation.</p> |
| 4 | <p>When you have finished administering the device, log out of the device. For network management servers or zone controllers, press Q until the initial login prompt appears. For other devices, log out accordingly.</p> <div data-bbox="488 953 586 1058"></div> <div data-bbox="612 976 846 1026">IMPORTANT</div> <p>Always log out of a device before disconnecting the session with the device or before closing out the terminal server session. Otherwise, the next user to log on with the device will resume where the previous session left off. Failure to do so will cause the administrative capabilities for the device to lock up.</p> <p>Result: The initial login prompt appears or the appropriate logout text appears.</p> |
| 5 | <p>After logging out of the device, press Ctrl+L to return to the submenu of the terminal server.</p> <div data-bbox="488 1365 586 1470"></div> <div data-bbox="612 1388 846 1438">NOTE</div> <p>After logging out of a device you can close the session with the device by using Procedure 4-10, "How to Disconnect a Session with a Device," on page 4-16. Always log out of a device before disconnecting its session.</p> |

Opening Sessions with a Number of Devices

Procedure 4-4 describes how you can open a number of simultaneous sessions with multiple devices.

Procedure 4-4 How to Open Sessions with a Number of Devices

1	<div>While in a session with one device, press Ctrl+L to return to the device submenu on the terminal server.</div> <div>Result: The device submenu on the terminal server is displayed.</div>
2	<div>Select another device from the submenu, or navigate to another submenu and select a device. To navigate to another submenu, press Shift+T to return to the main menu, then select another submenu.</div> <div>Result: A session with the newly selected device begins.</div>
3	<div>Press Enter until the login screen for the device appears.</div> <div>Result: The login prompt for the device appears.</div>
4	<div>Log on and administer the device.</div> <div><div><div>IMPORTANT</div><div>Do not forget to log out of each device before disconnecting device sessions from the terminal server or before closing out the terminal server session.</div></div><div><div>NOTE</div><div>To switch between multiple devices, press Ctrl+K or use Procedure 4-7, "How to Resume an Opened Device Session," on page 4-13. Pressing Ctrl+L returns to the terminal server menus, but does not disconnect the device session.</div></div></div>

Opening a Telnet Session with a Host

Procedure 4-5 describes how to open a Telnet session with a user-defined host through the terminal server.

Procedure 4-5 How to Open a Telnet Session with a User-Defined Host

1	<p>From the main menu, select Telnet Session to Host.</p> <p>Result: The following prompt is displayed: Telnet Session to Host...</p>
2	<p>Enter one of the following at the prompt:</p> <ul style="list-style-type: none"> • IP address of the appropriate device • IP address of the console port for devices not on the LAN <IP address of terminal server>:<port number assigned to device> <p>Result: A Telnet session with the device is opened.</p>
3	<p>If prompted, log on to the device.</p>
4	<p>When finished with the device, log out of the device.</p> <div data-bbox="483 968 586 1077"> </div> <div data-bbox="610 993 846 1041"> <p>NOTE</p> </div> <p>After logging out of a device, you can then close the session with the device by using Procedure 4-10, "How to Disconnect a Session with a Device," on page 4-16.</p>

Fixing Overlapping Lines in ProComm

Procedure 4-6 describes how to fix a problem that occurs when using ProComm to Telnet to a device.


Procedure 4-6 How to Fix Overlapping Lines in ProComm

1	<p>In ProComm, from the Options menu, select Data Options, and then select Terminal Options.</p>
2	<p>Select the Incoming CR to CR/LF check box and then click Apply.</p>
3	<p>When you have finished using this session, clear the Incoming CR to CR/LF setting or else the menus will overrun the screen.</p>

Resuming a Session with a Device

You can resume an open session with a device by selecting the session from a list of sessions as described in Procedure 4-7. You can also switch between sessions by pressing **Ctrl+K** until the desired session is resumed.

Procedure 4-7 How to Resume an Opened Device Session

1	<p>From the main menu, select Resume Session.</p> <p>Result: Text similar to the following is displayed:</p> <pre>Port 26: user1 Service Mode Current Session 1 - Session 1: Connected Interactive 10.1.233.222:2700 - Session 2: Connected Interactive 10.1.233.222:2800 - Session 3: Connected Interactive 10.1.233.222:2900</pre> <p>The following prompt is also displayed:</p> <pre>Resume Session...</pre>
2	<p>At the prompt, type the name of the session to be resumed from the list of opened device sessions, for example, <code>Session 1</code>, then press Enter.</p> <div><div>NOTE</div><p>If the resume session screen is displayed for more than 30 seconds, the terminal server resumes the first session from the list automatically.</p></div> <p>Result: The following prompt is displayed:</p> <pre>Press <Return> to continue...</pre>
3	<p>Press Enter to resume the session with the selected device.</p> <p>Result: A message similar to the following is displayed. You can then access and administer the device.</p> <pre>iTouch -012- 10.1.233.222:2900 session 3 resumed</pre>

Displaying All Remote Terminal Server Users

You can view all the users that are logged on to the terminal server by using Procedure 4-8. All users logged on to the terminal server are identified by the user names that they entered when they logged on to the terminal server.

Procedure 4-8 How to View All the Users Logged On to the Terminal Server

- 1 From the main menu, select **Show Users**.

Result: Text similar to the following is displayed.

Port	Username	Status	Port-Type	Service
2	(Remote)	Available	Console-Port	(Remote Connect)
3	(Remote)	Available	Console-Port	(Remote Connect)
4	(Remote)	Available	Console-Port	(Remote Connect)
5	(Remote)	Available	Console-Port	(Remote Connect)
6	(Remote)	Available	Console-Port	(Remote Connect)
7	(Remote)	Connected	Console-Port	(Remote Connect)
8	(Remote)	Available	Console-Port	(Remote Connect)
9	(Remote)	Available	Console-Port	(Remote Connect)
10	(Remote)	Available	Console-Port	(Remote Connect)
11	(Remote)	Available	Console-Port	(Remote Connect)
12	(Remote)	Available	Console-Port	(Remote Connect)
13	(Remote)	Available	Console-Port	(Remote Connect)
14	(Remote)	Available	Console-Port	(Remote Connect)
15	(Remote)	Available	Console-Port	(Remote Connect)
16	(Remote)	Available	Console-Port	(Remote Connect)
17	(Remote)	Available	Console-Port	(Remote Connect)
18	(Remote)	Available	Console-Port	(Remote Connect)
19	(Remote)	Available	Console-Port	(Remote Connect)
20	user1	Executing Cmd	Virtual-Port	10.1.233.222:2700

The following prompt is also displayed:
Press <Return> to continue...


Procedure 4-8 How to View All the Users Logged On to the Terminal Server (Continued)

2	After viewing the list, press Enter to view the remaining users logged on to the terminal server. Result: Any additional users are displayed.
3	Press Enter to return to the main menu. Result: The main menu is displayed.

Accessing the Terminal Server Maintenance Environment

You can access the terminal server maintenance environment through the main menu when logged on to the terminal server. Use Procedure 4-9 to access the terminal server maintenance environment.

Procedure 4-9 How to Access the Terminal Server Maintenance Environment

1	From the main menu, select Maintenance Access . Result: A <code>password></code> prompt appears.
2	Type the current maintenance password, then press Enter . Result: The terminal server maintenance environment is displayed. For example, the iTouch shows the <code>Priv></code> prompt.
	 <div style="background-color: #00AEEF; color: white; padding: 5px; display: inline-block;">NOTE</div> <p>Terminal server configuration instructions are provided in Volume 9, <i>Master Site Hardware and Software Configuration</i>. See your terminal server maintenance documentation for other specific commands and instructions that can be used for terminal server maintenance.</p>
3	When finished, use the appropriate commands to exit the maintenance environment. Type Logout to disconnect the session. Result: The session disconnects and the terminal server session closes. You must log back on to the terminal server if you have additional tasks to perform.

Disconnecting a Device Session

You can disconnect a session with a device by using Procedure 4-10.



NOTE

Be sure that you have logged out of the device before attempting to disconnect the session.

Procedure 4-10 How to Disconnect a Session with a Device

- 1** After logging out of the device, press **Ctrl+L** to return to the terminal server menu.

Result: The terminal server menu is displayed.

- 2** If a device submenu is currently displayed, press **Shift+T** to return to the main menu.

Result: The main menu is displayed.

- 3** From the main menu, select **Disconnect a Session**.

Result: Text similar to the following is displayed.

```
Port 26:  user1 Service Mode Current Session 1
- Session 1:  Connected Interactive 10.1.233.222:2700
- Session 2:  Connected Interactive 10.1.233.222:2800
- Session 3:  Connected Interactive 10.1.233.222:2900
```

The following prompt is also displayed:

Disconnect a Session...



CAUTION


The device must be logged out before you disconnect the device session in the next step. If you have not logged out of the device (as instructed in step 1), press **Ctrl+K** and log out of the device at this time. Failure to log out of a device will cause the administrative capability of that device to lock up, and may require a reset to free the administrative capabilities for the device.



NOTE

If a session is not chosen within 30 seconds, the first session from the list is disconnected automatically.

Procedure 4-10 How to Disconnect a Session with a Device (Continued)

4	<p>At the prompt, type the name of the session to be disconnected, for example, Session 1, then press Enter.</p> <div data-bbox="386 359 488 468"></div> <div data-bbox="513 384 748 434">NOTE</div> <p>To disconnect all the listed sessions, type ALL at the prompt, then press Enter.</p> <p>Result: The following prompt is displayed: Press <Return> to continue...</p>
5	<p>Press Enter to disconnect the selected session(s).</p> <p>Result: The selected session(s) are disconnected and the main menu is displayed.</p>

Logging Out of the Terminal Server

Procedure 4-11 describes how to safely log out of the terminal server.

**CAUTION**

Before logging out of the terminal server, ensure that you have logged out of all devices and disconnected all device sessions. Failure to do so will cause the administrative capabilities of these devices to lock up. See Procedure 4-10, "How to Disconnect a Session with a Device," on page 4-16 for instructions on disconnecting a device session.

Procedure 4-11 How to Log Out of the Terminal Server

1	<p>After logging out of all devices and disconnecting all device sessions, press Shift+Q to log out of the terminal server.</p> <p>Result: The client logs out of the terminal server, and the Telnet session is terminated.</p>
2	<p>Close the window.</p> <p>Result: The window closes.</p>

Viewing the Remote Terminal Server Configuration

Procedure 4-12 describes how to view the remote terminal server configuration.

Procedure 4-12 How to View the Remote Terminal Server Configuration

1	From the main menu, select Maintenance Access . Result: A <code>password></code> prompt is displayed:																
2	Type the current maintenance password, then press Enter . Result: The terminal server maintenance environment is displayed																
3	Type the following commands in any order to view the configuration information:																
4	<table> <tr> <th>IF you want to view:</th><th>THEN:</th></tr> <tr> <td>All IP information</td><td>Type sh ip ch and press Enter.</td></tr> <tr> <td>All port information</td><td>Type sh port ch and press Enter.</td></tr> <tr> <td>Software version</td><td>Type sh man files and press Enter.</td></tr> <tr> <td>Configuration of ports</td><td>Type sh port <number> ppp stat and press Enter.</td></tr> <tr> <td>Current port characteristics, what is enabled or disabled</td><td>Type sh port alt ch and press Enter.</td></tr> <tr> <td>Values on a specific port</td><td>Type sh port <number> alt ch and press Enter.</td></tr> <tr> <td>Current status of a port</td><td>Type sh port <number> stat and press Enter.</td></tr> </table>	IF you want to view:	THEN:	All IP information	Type sh ip ch and press Enter .	All port information	Type sh port ch and press Enter .	Software version	Type sh man files and press Enter .	Configuration of ports	Type sh port <number> ppp stat and press Enter .	Current port characteristics, what is enabled or disabled	Type sh port alt ch and press Enter .	Values on a specific port	Type sh port <number> alt ch and press Enter .	Current status of a port	Type sh port <number> stat and press Enter .
IF you want to view:	THEN:																
All IP information	Type sh ip ch and press Enter .																
All port information	Type sh port ch and press Enter .																
Software version	Type sh man files and press Enter .																
Configuration of ports	Type sh port <number> ppp stat and press Enter .																
Current port characteristics, what is enabled or disabled	Type sh port alt ch and press Enter .																
Values on a specific port	Type sh port <number> alt ch and press Enter .																
Current status of a port	Type sh port <number> stat and press Enter .																
5	When finished, type Logout to disconnect the session. Result: The session disconnects and the terminal server session closes. You must log back on to the terminal server if you have additional tasks to perform.																

Backing Up and Restoring the Remote Terminal Server

This section contains the following backup and restore procedures that apply to both the iTouch and Xyplex terminal servers:

- "Backing Up the Terminal Server OS, Parameter File, and Menu File" on page 4-20

- "Restoring the Terminal Server OS, Parameter File, and Menu File" on page 4-24

**NOTE**

For connectivity to the remote terminal server, and the configuration table information, see Volume 9, *Master Site Hardware and Software Configuration*.

Backing Up the Terminal Server OS, Parameter File, and Menu File

The terminal server files can be backed up using a TFTP GET command. Follow Procedure 4-13 to back up these files using a PC and the 3CServer TFTP application.

**NOTE**

To install the 3Com TFTP Server software, see "Installing the 3Com TFTP Server Software" on page 5-7.

The following files must be backed up:

- MCFFS1 — the load file.
- NEMC_IR.SYS — the iTouch terminal server image file operating system.
- XPCSRV20.SYS — the Xyplex terminal server image file operating system.
- -806EB1.SYS — compiled parameter file. (The file name is derived from the MAC address; therefore, every terminal server has a unique parameter file name.)
- DEFAULT.SYS — the factory defaults file.


- MENU.TXT — nested menu text file (iTouch Out-of-Band Management terminal servers only).



NOTE

Your process may differ if you are using a TFTP application other than the 3CServer.

Procedure 4-13 How to Back Up Terminal Server Files

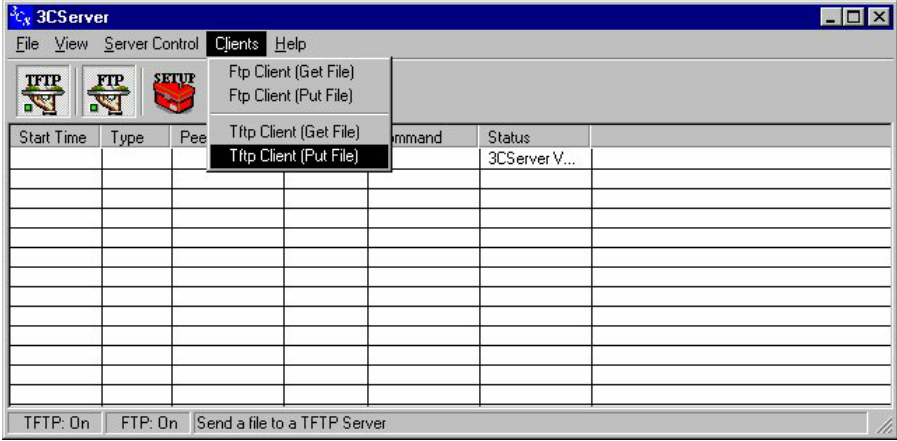
1	<p>From the main menu, select Maintenance Access.</p> <p>Result: A <code>password></code> prompt is displayed.</p>																																			
2	<p>Type the current maintenance password, then press Enter.</p> <p>Result: The terminal server maintenance environment is displayed.</p>																																			
3	<p>From the <code>privileged</code> mode CLI, type show man files and press Enter.</p> <p>Result: The names of the files that need to be backed up appear. This example shows iTouch files.</p> <pre>IR8020 V2.3 Rom 460000 HW 00.00.00 Lat Protocol V5.2 Uptime: 0 00:06:53 Address: 08-00-87-80-6E-B1 Name: ITOUCH_A Number: 0 17 APR 2001 00:06:53</pre> <p>Files from directory /MC/SYSTEM</p> <table><thead><tr><th>File Name</th><th>Version</th><th>Date</th><th>Time</th><th>Size</th></tr></thead><tbody><tr><td>MCFFS1.SYS</td><td>V2.22</td><td>17 Apr 2001</td><td>13:34:30</td><td>29248 bytes AREA 1 Size 64856</td></tr><tr><td>NEMC_IR.SYS</td><td>V2.3</td><td>17 Apr 2001</td><td>13:35:28</td><td>920256 bytes AREA 2 Size 3079217</td></tr></tbody></table> <p>2 files, 949504 bytes.</p> <p>Files from directory /MC/PARAM</p> <table><thead><tr><th>File Name</th><th>Version</th><th>Date</th><th>Time</th><th>Size</th></tr></thead><tbody><tr><td>-806EB1.SYS</td><td>ver 38</td><td>17 Apr 2001</td><td>00:00:36</td><td>11406 bytes</td></tr><tr><td>DEFAULTS.SYS</td><td>ver 0</td><td>17 Apr 2001</td><td>13:34:02</td><td>1024 bytes</td></tr><tr><td>MENU.TXT</td><td>-none-</td><td>17 Apr 2001</td><td>01:30:20</td><td>1815 bytes</td></tr></tbody></table> <p>3 files, 14245 bytes.</p>	File Name	Version	Date	Time	Size	MCFFS1.SYS	V2.22	17 Apr 2001	13:34:30	29248 bytes AREA 1 Size 64856	NEMC_IR.SYS	V2.3	17 Apr 2001	13:35:28	920256 bytes AREA 2 Size 3079217	File Name	Version	Date	Time	Size	-806EB1.SYS	ver 38	17 Apr 2001	00:00:36	11406 bytes	DEFAULTS.SYS	ver 0	17 Apr 2001	13:34:02	1024 bytes	MENU.TXT	-none-	17 Apr 2001	01:30:20	1815 bytes
File Name	Version	Date	Time	Size																																
MCFFS1.SYS	V2.22	17 Apr 2001	13:34:30	29248 bytes AREA 1 Size 64856																																
NEMC_IR.SYS	V2.3	17 Apr 2001	13:35:28	920256 bytes AREA 2 Size 3079217																																
File Name	Version	Date	Time	Size																																
-806EB1.SYS	ver 38	17 Apr 2001	00:00:36	11406 bytes																																
DEFAULTS.SYS	ver 0	17 Apr 2001	13:34:02	1024 bytes																																
MENU.TXT	-none-	17 Apr 2001	01:30:20	1815 bytes																																
	<div><div>NOTE</div></div> <p>To see the full list of files, press Enter. You should write down the file names or keep the session window open in the background. On the list of file names, the Date and Time fields will appear as “0”s and “?”s if the NTP server has not yet been updated.</p>																																			
4	<p>Connect an Ethernet crossover cable from the PC to the terminal server using the Ethernet port, or use two straight-through cables and connect them to a hub or switch.</p>																																			
5	<p>To verify that the PC’s IP address is within the same subnet of the terminal server’s IP address, open a Command Prompt window, type ipconfig, and press Enter. If not, modify the PC’s IP address so that it is within the terminal server’s IP subnet (for example, 10.1.233.0).</p>																																			



NOTE

To see the full list of files, press **Enter**. You should write down the file names or keep the session window open in the background. On the list of file names, the Date and Time fields will appear as "0"s and "?"s if the NTP server has not yet been updated.

Procedure 4-13 How to Back Up Terminal Server Files (Continued)

6	Ping the terminal server to verify network connectivity. From a command prompt window, verify ping by typing ping xxx.xxx.xxx.xxx and wait for the ping reply.
7	<p>Open the 3CServer TFTP server application, using one of the following methods:</p> <ul style="list-style-type: none">• Right-click the 3CS icon on the toolbar and select the Show Window option.• From the Start button, select Programs, and then select 3CServer. <p>Result: The 3CServer window appears (Figure 4-4).</p> <p>Figure 4-4 3CServer Window</p> 
8	<p>From the Clients menu, select TFTP Client (Get File).</p> <p>Result: The TFTP Get File Information dialog box appears.</p>

Procedure 4-13 How to Back Up Terminal Server Files (Continued)**9**

You have to back up four files. Complete the fields as indicated in the following example:

TFTP Host: xxx.xxx.xxx.xxx (terminal server's IP address)

Port: 69 (do not change this value)

Load File Example:

Remote file name: /mc/system/mcffs1.SYS_secure

(directory/filename_privileged password)

Local file name: C:\temp\mcffs1.SYS (location of menu file)

OS File Example:

Remote file name: /mc/system/nemc_ir.SYS_secure

(directory/filename_privileged password)

Local file name: C:\temp\nemc_ir.SYS (location of menu file)

**NOTE**

The Xyplex models use the XPCSRV20.SYS file name for the above OS file example.

Parameter File Example:

Remote file name: /mc/param/-806EB1.SYS_secure

Local file name: C:\temp\ -806EB1.SYS

Menu File Example:

Remote file name: /mc/param/menu.txt_secure

Local file name: C:\temp\menu.txt

**NOTE**

To see the full list of files, press **Enter**.

**NOTE**

If the correct privileged password is not appended to the file name, the operation will fail. Some TFTP server applications are sensitive about the file name length. Keep the file names as short as possible to avoid problems.

10

Click **OK** when you have finished completing the fields.

Result: The Status column of the 3CServer window shows TFTP: Successful when the transfer is complete. The files are saved to the hard drive; you can browse to view the location of the files.

Restoring the Terminal Server OS, Parameter File, and Menu File

Process 4-1 describes the restore process.



Process 4-1 Restoring the Terminal Server OS, Parameter File, and Menu File

1	Bring the terminal server to the minimum factory settings. See "Restoring Factory Defaults" on page 4-24.
2	Restore the parameter and menu files from the factory defaults. See "Restoring the Parameter and Menu Files from Factory Defaults" on page 4-26.
3	Restore the load and image files. See "Upgrading/Restoring the Load and Image Files" on page 4-29.


Restoring Factory Defaults

Follow Procedure 4-14 to restore the terminal server to factory defaults.

Procedure 4-14 How to Restore Terminal Server to Factory Defaults

1	<p>At the <code>priv ></code> prompt, type REMOVE "/mc/param/menu.txt" and then press Enter.</p> <div>  <div> IMPORTANT <p>Before setting factory defaults, you must remove the menu.txt file in the flash card. You can issue show man files to verify that the file is gone.</p> </div> </div>
2	Plug a terminal into the highest-numbered serial port on the terminal server to access the Initialization menu.
3	<p>Press the Reset button once.</p> <div>  <div> NOTE <p>The Reset button is recessed and found to the right of the Console LED on the front panel of the terminal server. Use a straightened paper clip to press the button.</p> </div> </div> <p>Result: All LEDs on the front panel illuminate.</p>
4	<p>Press and hold down the Reset button again.</p> <p>Result: While pressing the Reset button, observe the port LEDs. The port LEDs should extinguish first, then illuminate in sequence from left to right. Wait for all LEDs to extinguish in sequence from left to right.</p>

Procedure 4-14 How to Restore Terminal Server to Factory Defaults (Continued)

5	<p>When the sequence has completed, release the Reset button. When the Run LED blinks rapidly (indicating that the self-test has completed), autobaud any serial port by pressing Enter a few times at a terminal connected to the port.</p> <p>Result: A message similar to the following displays: CONFIGURATION IN PROGRESS. PLEASE WAIT.</p>
6	<p>Type the default password: ACCESS. Press Enter.</p> <div data-bbox="483 510 586 619">  </div> <div data-bbox="610 537 846 583" style="background-color: #00AEEF; color: white; padding: 5px; text-align: center;">NOTE</div> <p style="text-align: center;">No prompt is displayed.</p> <p>Result: The Initialization menu is displayed.</p> <pre>Welcome to the Initialization Configuration Menu. In-Reach Configuration Menu 1. Display unit configuration 2. Modify unit configuration 3. Initialize server and port parameters 4. Revert to stored configuration S. Exit saving configuration changes X. Exit without saving configuration changes Enter menu selection [X]:</pre>
7	<p>Select 2, Modify Unit Configuration.</p> <p>Result: The Modify Unit Configuration menu displays.</p> <pre>Modify Unit Configuration Menu 1. Initialization record #1 (Enabled) 2. Initialization record #2 (Disabled) 3. Initialization record #3 (Disabled) M. Miscellaneous unit configuration D. Set unit configuration to defaults X. Exit to main menu Enter menu selection [X]:</pre>
8	<p>Select 1, Initialization record #1.</p> <p>Result: The Set Initialization Record #1 to defaults prompt appears.</p>
9	<p>Press Y, and then press Enter.</p> <p>Result: The Enable Initialization Record #1 prompt appears.</p>
10	<p>Press Y, and then press Enter. Press any key to continue.</p> <p>Result: The Modify Unit Configuration menu displays.</p> <pre>Modify Unit Configuration Menu 1. Initialization record #1 (Enabled) 2. Initialization record #2 (Disabled) 3. Initialization record #3 (Disabled) M. Miscellaneous unit configuration D. Set unit configuration to defaults X. Exit to main menu Enter menu selection [X]:</pre>

Procedure 4-14 How to Restore Terminal Server to Factory Defaults (Continued)

11	<p>Press D, Set Unit Configuration to Defaults, and then press Enter.</p> <p>Result: The following prompt displays: Initialize ALL configuration data for this unit to defaults (Y,N) [N]?</p>
12	<p>At the Initialize ALL configuration data for this unit to defaults prompt, press Y and then press Enter.</p> <p>Result: The Modify Unit Configuration menu displays again.</p>
13	<p>Press X to exit to the main menu and then press Enter.</p> <p>Result: The Server Configuration menu displays. In-Reach Server Configuration Menu 1. Display unit configuration 2. Modify unit configuration 3. Initialize server and port parameters 4. Revert to stored configuration S. Exit saving configuration changes X. Exit without saving configuration changes Enter menu selection [X]:</p>
14	<p>Select option 3, Initialize server and port parameters, and then press Enter.</p> <p>Result: The following message displays: When the software has been loaded, should default server and port parameters be used (Y,N)</p>
15	<p>Press Y to use the default server and port parameters, and then press Enter.</p> <p>Result: The Server Configuration menu displays.</p>
16	<p>Press S, Exit saving configuration changes and then press Enter.</p> <p>Result: The following message appears: WARNING! Server and port parameters will be re-set to initial values. (Type any key to continue)</p>
17	<p>Press any key to continue.</p> <p>Result: The following message appears: Save changes and exit (Y,N) [Y]?</p>
18	<p>Press Y at the prompt and press Enter.</p> <p>Result: The terminal server reboots. Wait approximately five minutes. When the reboot is complete, the terminal server is restored to factory defaults. The reboot is complete when the green RUN LED flickers, the LAN LED is illuminated, and no amber LEDs are illuminated.</p>

Restoring the Parameter and Menu Files from Factory Defaults

To restore the terminal server from factory defaults, the files must be transferred using the TFTP PUT command. The first file transferred is the MAC addressed parameter file. Once the file has been transferred and the terminal server has been rebooted, the menu file can then be transferred.

Follow Procedure 4-15 to restore the terminal server.

Procedure 4-15 How to Restore Files from Factory Defaults

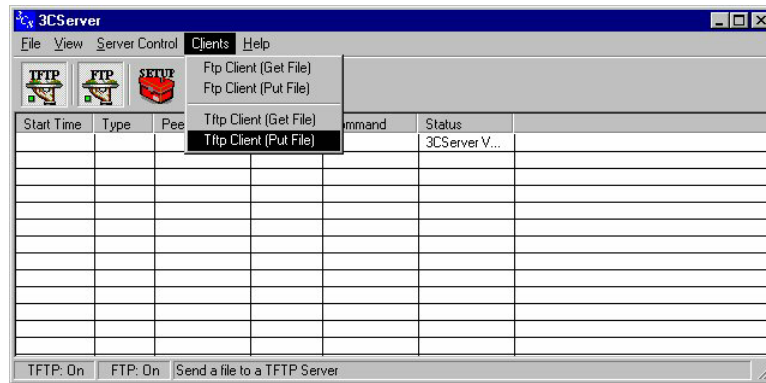
1	<p>Log on to the terminal console port (the highest-numbered serial port) using the default login and privileged mode passwords (access, system).</p> <ol style="list-style-type: none"> 1. Press Enter a couple of times to access the prompt. <p>Result: The <code>Login></code> prompt appears.</p> <ol style="list-style-type: none"> 2. Type access and press Enter. <ul style="list-style-type: none"> • For the iTouch, the welcome screen appears, followed by the <code>Enter Username></code> prompt. Enter a name at the prompt. At the <code>iTouch></code> prompt, type the following command to enter the privileged mode: <code>iTouch> set pri</code> and press Enter. At the <code>Password></code> prompt, type system. • For the Xyplex, the privileged mode prompt appears. <p>Result: The privileged mode prompt, <code>iTouch_priv></code> or <code>Xyplex>></code> appears.</p>
2	<p>Define the IP address and subnet mask of the terminal server with the following commands. You may have different IP addresses according to your System ID and Zone ID, so the following is an example:</p> <p>iTouch Terminal Servers:</p> <pre>DEFINE SERVER IP ADDRESS 10.1.233.222 DEFINE SERVER IP SUBNET MASK 255.255.255.0</pre> <p>Xyplex Terminal Servers:</p> <pre>SET SERVER IP ADDRESS 10.1.233.222 SET SERVER IP SUBNET MASK 255.255.255.0</pre>
3	<p>Type show server ip and press Enter to verify the settings.</p>
4	<p>Type ping 10.1.233.222 and press Enter.</p> <p>Result: The result shows connectivity to the terminal server.</p>

Procedure 4-15 How to Restore Files from Factory Defaults (Continued)

- 5** Open the 3CServer TFTP server application by one of the following methods:
- Right-click the **3CS** icon on the toolbar and select the **Show Window** option.
 - From the **Start** button, select **Programs**, and then select **3CServer**.

Result: The 3CServer window appears (Figure 4-5).

Figure 4-5 3CServer Window



- 6** From the Clients menu, select **TFTP Client (Put File)**.

Result: The TFTP Put File Information dialog box appears.

- 7** Complete the fields as indicated in the following example, and then click **OK**.
- TFTP Host: **xxx.xxx.xxx.xxx** (terminal server's IP address)
 - Port: **69** (do not change this value)
 - Remote file name: **/mc/param/-806EB1.SYS_system**
 - Local file name: **C:\temp\806EB1.SYS**



IMPORTANT

The compiled backup parameter file may be used in a new or different terminal server. If so, the remote file name is different. To obtain the file name of the new or different terminal server, type the **show man files** command. The file name is always under the **/mc/param/** directory. The following example shows how to restore the backup parameter file into a new terminal server:

- Remote file name: **/mc/param/-866818.SYS_system**
- Local file name: **C:\temp\806EB1.SYS**

Result: The file transfers.

Procedure 4-15 How to Restore Files from Factory Defaults (Continued)

8	<p>After the file has transferred, from the privileged mode, type the following command: COPY "/MC/PARAM/-806EB1.SYS" NVS</p> <p>Result: A prompt appears to press the CR. Press Enter and the terminal server reboots.</p> <div data-bbox="483 436 586 537"> </div> <div data-bbox="610 457 846 506"> <p>NOTE</p> </div> <p>The terminal server reboot takes approximately five minutes. The following steps apply to transferring a nested menu file for iTouch terminal servers used for out-of-band management. You do not need to follow this procedure if you are using a Xyplex terminal server or an iTouch 4 or 8 port terminal server for remote analog access.</p>
9	<p>Log on to the terminal server using the passwords stored in the parameter file.</p> <ol style="list-style-type: none"> 1. Press Enter a few times to access the LOGIN> prompt. This uppercase prompt indicates the parameter file transferred successfully. 2. Type motorola and press Enter. <p>Result: The Enter Username> prompt appears.</p> <ol style="list-style-type: none"> 3. Enter a name. 4. At the iTouch> prompt, type set pri secure and press Enter. The privileged mode prompt appears.
10	<p>Transfer the archived or updated menu file to the terminal server using the TFTP PUT client:</p> <ul style="list-style-type: none"> • TFTP Host: xxx.xxx.xxx.xxx (terminal server's IP address) • Port: 69 (do not change this value) • Remote file name: /mc/param/menu.txt_secure • Local file name: C:\temp\menu.txt
11	<p>To reboot the terminal server, at the privileged prompt, type INIT DELAY 1 and press Enter. Press Enter at all Press Enter to Continue prompts.</p> <p>Result: The privileged prompt appears, and the terminal server reboots and is ready for use after approximately five minutes.</p>

Upgrading/Restoring the Load and Image Files

This procedure is used for an upgrade or to restore the files.



NOTE

It is highly unlikely that these files will need to be restored. Restore the files only at the request of the Motorola System Support Center. The more likely scenario of using this procedure would be if the terminal server required an upgrade of these files.

Follow Procedure 4-16 to upgrade or re-install the image and load files.

Procedure 4-16 How to Upgrade/Restore Load and Image Files

1	<p>Set up the TFTP Upload and Download directory that contains the image and load files.</p> <ol style="list-style-type: none"> 1. In the TFTP main window, click the Setup icon. 2. In the setup window, change the Upload/Download directory to C:\temp\.
2	<p>Log on to the terminal server .</p> <ol style="list-style-type: none"> 1. Press Enter a few times to access the LOGIN> prompt. 2. Type motorola and press Enter. The <code>Enter Username></code> prompt appears. 3. Enter a name. <p>Result: The Main Menu appears.</p>
3	<p>Select Option 1, Maintenance Access.</p> <p>Result: The privileged prompt appears.</p>
4	<p>Obtain the area parameter and version number of the files to be upgraded/restored by using the SHOW MAN FILES command.</p> <div data-bbox="391 1163 488 1268"> </div> <div data-bbox="574 1192 685 1232" data-label="Section-Header"> <h2>NOTE</h2> </div> <p>For an example of using the Show Man Files command, see Procedure 4-13, "How to Back Up Terminal Server Files," on page 4-20.</p> <p>Result: A list of files displays. Note the areas and version numbers.</p>

Procedure 4-16 How to Upgrade/Restore Load and Image Files (Continued)

- 5** Issue the following commands from the privileged mode CLI on the terminal server:

**NOTE**

The IP address in the following commands refers to the IP address of the TFTP server/PC.

```
GET CARD LOAD FILE "MCFFS1.SYS" IP ADDRESS
10.1.233.249 AREA 1
```

iTouch Terminal Servers:

```
GET CARD LOAD FILE "NEMC_IR.SYS" IP ADDRESS
10.1.233.249 AREA 2
```

Xyplex Terminal Servers:

```
GET CARD LOAD FILE "XPCSRV20.SYS" IP ADDRESS
10.1.233.249 AREA 2
```

- 6** Type **SHOW CARD STATUS** from the privileged mode CLI on the terminal server.

Result: The following message displays:

```
GET FILE PREVIOUS STATUS: GET FILE COMPLETED SUCCESSFULLY
```

**NOTE**

If you do not receive the above message, keep issuing the **SHOW CARD STATUS** command until you receive the expected message. If after several minutes this status does not appear, you may have to repeat the previous step and reissue the **GET** commands.

- 7** Issue the **SHOW MAN FILES** command and verify that the new files have been successfully copied to the flashcard and that the file sizes match the original decompressed files on the host.

- 8** To reboot the terminal server, type **INIT DELAY 1** from the privileged mode CLI and press **Enter**. Press **Enter** at all **Press Enter to Continue** prompts.

Result: Wait approximately five minutes for the terminal server to reboot.

This page intentionally left blank.

Managing Other Transport Equipment

This chapter provides the following information to manage network transport equipment other than the LAN switch, WAN switch, routers, and remote terminal server.



NOTE

An ASTRO 25 SE system does not contain the Cisco Catalyst 6509 Ethernet LAN switch (LAN switch) or Nortel Passport 7480 WAN switch (WAN switch). Ignore all references to these switches. This chapter includes the following topics:

- "Managing Configuration Data" on page 5-1
- "Backing Up Configuration Data" on page 5-2
- "Common Setup Procedures" on page 5-3
- "Managing the ARCA-DACS" on page 5-10
- "Managing the Channel Bank" on page 5-25
- "Managing the Digital Service Unit/Channel Service Unit" on page 5-32
- "Managing the HP Procurve Ethernet Switch" on page 5-33
- "Managing the Modem" on page 5-38
- "Managing the TRAK 9100" on page 5-40

Managing Configuration Data

All of the devices that provide network connectivity require the input of configuration data for proper operation. This can range from providing the IP address for a network device so that it can be managed by the system, to performing extensive configuration of a router so that it can intelligently route data between source and destination.

This chapter provides procedures to back up and restore network transport device configuration information. These procedures are designed to circumvent the re-entering of configuration data from the very initial configuration steps. However, if you find you must start from the beginning, see Volume 9, *Master Site Hardware and Software Configuration*.

**IMPORTANT**

If there is a problem, call your local Motorola® Field Representative. You should not add anything to or delete anything from the LAN/WAN. All additions and deletions must be performed by Motorola Field Representatives.

This chapter also provides the details of properly backing up and restoring the configuration data for the following network devices:

- ARCA-DACS™
- Channel bank
- Digital Service Unit/Channel Service Unit
- Ethernet switch
- Modem
- TRAK 9100

Several of the backup and restore procedures use programs that allow the PC (usually a laptop) to connect to the device either via a serial port or through an Ethernet LAN. See "Common Setup Procedures" on page 5-3 for program details.

Backing Up Configuration Data

Maintaining backups of the most current configuration for every network device in your system is critical. Current backups are necessary for reloading the configuration information if a device fails and must be replaced, or if the data stored in the device has somehow been lost.

**IMPORTANT**

Only restore the configuration information if there is a problem with a device due to failure or lost data, and you want to revert to a previous configuration.

Three-Copy Backup Rule

Acceptable media for the backups include:

- A spare device
- Paper (hard copy)
- CD-R, floppy disk

- Hard drive
- Optical drive

Table 5-1 provides a list of backup media recommendations for network transport devices.

Table 5-1 List of Backup Media Recommendations for Network Transport Devices

Backup Media	Network Transport Devices Using this Media
Hard drive	ARCA-DACS, Channel bank
Paper (hard copy)	Digital Service Unit/Channel Service Unit, Ethernet Switch, Modem

Regardless of the media chosen, it is recommended to use three media sources as follows:

- One for storage with the device
- One for on-site archiving
- One for off-site archiving

Common Setup Procedures

This booklet uses the Microsoft® HyperTerminal terminal emulator and/or the Trivial File Transfer Protocol (TFTP) server application in several backup and restore procedures.



NOTE

The backup command creates a simple text file. The actual commands for the backup procedure may vary depending on the computer and terminal emulator software you use to interface with the system.

Setting Up Microsoft HyperTerminal Software

Follow Procedure 5-1 to set up the Microsoft HyperTerminal software. (You could also use ProComm or another VT100 emulation program.) The following equipment requires Microsoft HyperTerminal software:

- Ethernet switch

- Channel bank

Procedure 5-1 How to Set Up Microsoft HyperTerminal

1	Look on your PC for Microsoft HyperTerminal. If you do not have it installed, connect to the Internet and go to the following website: http://download.cnet.com/
2	Search for HyperTerminal, download the application to your PC, and then install the application to Start\Programs\Accessories.
3	On the taskbar, click Start , then select Programs . Select the folder that contains Accessories , then select the folder that contains HyperTerminal , and then select HyperTerminal . Result: The Microsoft HyperTerminal application opens with the Connection Description dialog box (Figure 5-1).

Figure 5-1 Connection Description Dialog Box

Procedure 5-1 How to Set Up Microsoft HyperTerminal (Continued)

- 4** In the **Name** box, enter the name of the connection (in this example, “9600”), and in the **Icon** box click any icon other than the one with the red telephone (in this example, the “GE” icon). Click **OK**.

Result: The Connection Description is complete. The Connect To dialog box appears (Figure 5-2).

Figure 5-2 Connect To Dialog Box

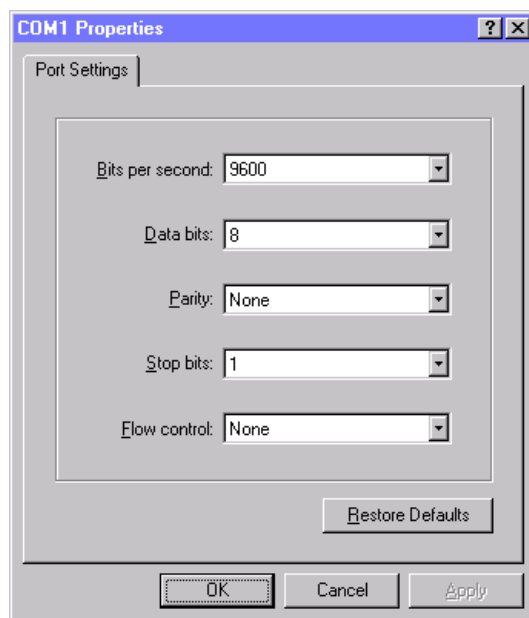


- 5** In the Connect using drop-down list, select **COM1** and click **OK**.

Result: COM1 is selected as the serial communications port on the computer. The physical connection on the computer is usually made at a DB9 jack. The COM1 Properties dialog box appears.

Procedure 5-1 How to Set Up Microsoft HyperTerminal (Continued)

- 6** Select the **Port Settings** tab (Figure 5-3), and select the following options:
- In the Bits per second drop-down list, select **9600** (or the appropriate baud rate).
 - In the Data bits drop-down list, select **8**.
 - In the Parity drop-down list, select **None**.
 - In the Stop bits drop-down list, select **1**.
 - In the Flow control drop-down list, select **None**.

Figure 5-3 Port Settings Tab

- 7** Click **OK**.

Result: The COM1 properties are programmed correctly.

Procedure 5-1 How to Set Up Microsoft HyperTerminal (Continued)

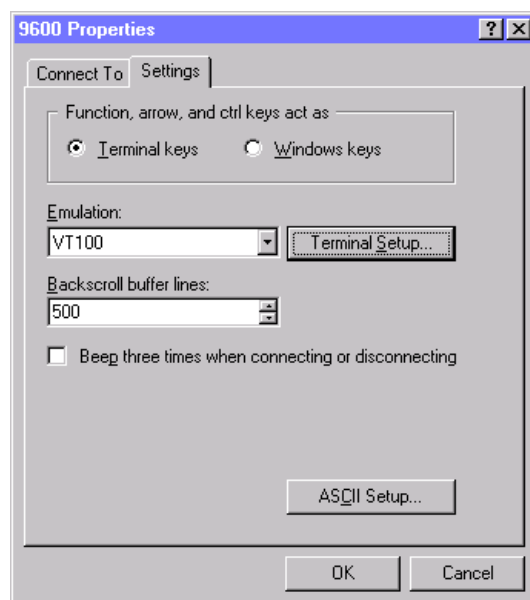
8 On the File menu, select **Properties**.

Result: The connection properties dialog box (in this example, it is 9600 Properties) appears.

9 Select the **Settings** tab (Figure 5-4). In the **Emulation** drop-down list, select **VT100**. Click **OK**.

Result: The COM1 port is configured for VT100 emulation.

Figure 5-4 Settings Tab



Installing the 3Com TFTP Server Software

Procedure 5-2 describes how to install the 3Com® TFTP server (3CServer) application software. If you use a TFTP server application other than 3Com, the command syntax might be different. The following equipment requires 3CServer software:

- ARCA-DACS

- Ethernet switch

Procedure 5-2 How to Install 3Com TFTP Server

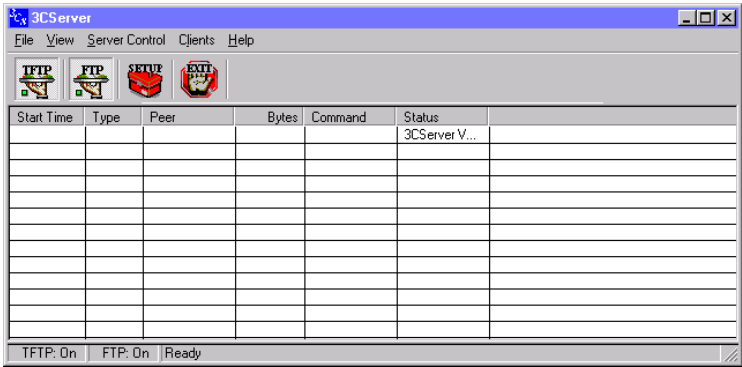
1

Look on your PC for the **3CServer.exe** file. If you do not have it installed, connect to the Internet and go to the following website:
<http://www.3com.com/index2.html>
Search for **3cs117.zip**, and click on the first product displayed. Find the **3cs117.zip** file under Downloads, and download the application to your PC. Extract and install the application on your PC.

2

Double-click on the **3CServer.exe** file to open the application.
Result: The 3CServer window appears (Figure 5-5).

Figure 5-5 3CServer Window



3

Look on your PC for Microsoft HyperTerminal. If you do not have it installed, see "Setting Up Microsoft HyperTerminal Software" on page 5-3.
Result: Both Microsoft HyperTerminal and 3CServer are open.

4

Ensure that your PC has an IP address, write it down, and save it for future use.

5

Configure the TFTP settings. See "Setting Up TFTP" on page 5-9.

Setting Up TFTP

Procedure 5-3 describes how to set up the TFTP settings that you use to backup and restore the ARCA-DACS and the Ethernet switch.

Procedure 5-3 How to Set Up TFTP

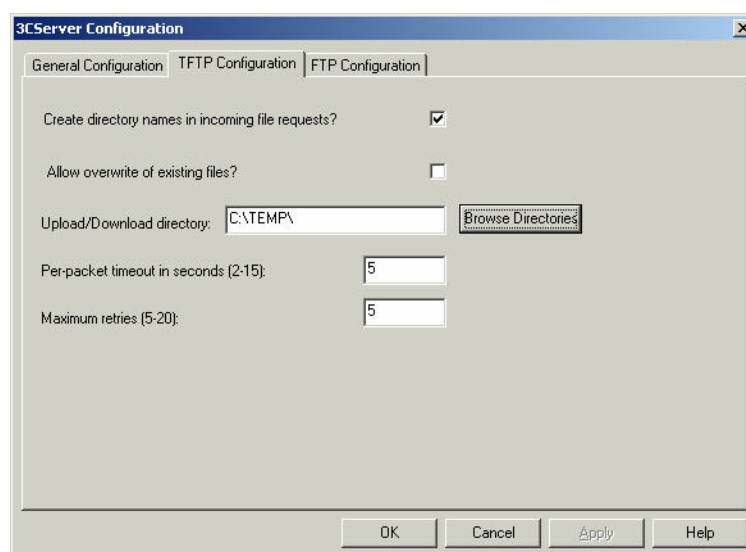
1

On the 3CServer application window, click the **Setup** icon.



Result: The 3CServer Configuration dialog box appears.

Figure 5-6 3CServer Configuration



2

Select the **TFTP Configuration** tab and choose the following settings:

- Select the **Create directory names in incoming file requests** check box.
- (Optional) Clear the **Allow overwrite of existing files?** check box.
- In the Upload/Download directory box, browse to the directory path.
- In the Per-packet timeout in seconds (2-15) box, type **15**.
- In the Maximum retries (5-20) box, type **20**.

3

Click **OK**.

Managing the ARCA-DACS

This section describes how to view the configuration of the ARCA-DACS 100 Scaleable Digital Access and Cross-Connect System (ARCA-DACS), then how to back up or restore the data.

This section does **not** discuss how to configure the ARCA-DACS. See Volume 9, *Master Site Hardware and Software Configuration* or www.zhone.com for configuration information.

You can find additional information at www.zhone.com and in the following Zhone® Technologies manuals that ship with the ARCA-DACS:

- **Configuration Management Tool, SECTOR 300 & ARCA-DACS 100,**
Release 2.5.2, User's Guide
CMT for Windows NT, Release 2.5.2, Release Notes



NOTE

These procedures use the vendor supplied, Configuration Management Tool (CMT™) software for NT, release 2.5.2.

Your ASTRO 25 system may not have an ARCA-DACS. The only time a system requires an ARCA-DACS is if there are analog mutual aid stations located at remote sites. The ARCA-DACS combines the analog mutual aid voice, ASTRO 25 voice, and digital control onto a T1 going out to remote sites.

Viewing the ARCA-DACS Configuration

Procedure 5-4 describes how to view the ARCA-DACS configuration parameters.

**NOTE**

The CMT application must be installed before performing this procedure. See "Installing the Configuration Management Tool Software" on page 5-14.

Procedure 5-4 How to View the ARCA-DACS Configuration

- 1** Double-click the **CMT2.5.2** desktop shortcut icon to open the CMT application.
Result: The CMT Login dialog box appears (Figure 5-7).

Figure 5-7 CMT Login Dialog Box

The screenshot shows a window titled "CMT Login". It has four input fields: "IP Address/Name", "User Name", "Password", and "TimeOut (mins)". To the right of the "TimeOut (mins)" field is a checkbox labeled "Enable TimeOut". Below these fields is another checkbox labeled "Set Sechtor's time using this machine's time.". At the bottom of the window are two buttons: "OK" and "Quit".

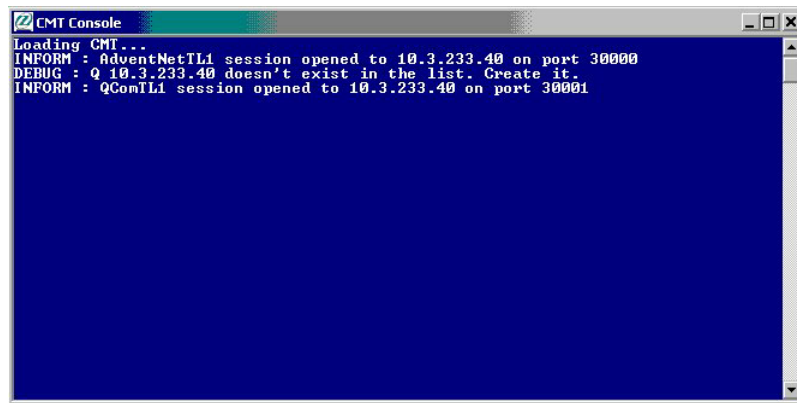
- 2** Do the following to log on:
1. In the **IP Address/Name** box, type the IP address of the ARCA-DACS (using the format **nnn.nnn.nnn.nnn**, where **nnn** = (0-255) (for example, "43.166.199.23")), and press **Tab**.
 2. In the **User Name** box, type the user name and press **Tab**. (If the ARCA-DACS is not provisioned, type **ROOT**; it is case-sensitive.)
 3. In the **Password** box, type the password (for root-level access, type the default password, **factory1%**) and press **Tab**.
 4. In the **TimeOut (mins)** box, type the TimeOut time that you want, for example, 30 minutes and press **Tab**.
 5. Select the **Enable TimeOut** check box.
 6. Do **not** select the Set Sechtor's time using this machine's time check box because NTP time setting will not take effect.

Procedure 5-4 How to View the ARCA-DACS Configuration (Continued)

3 Click **OK**.

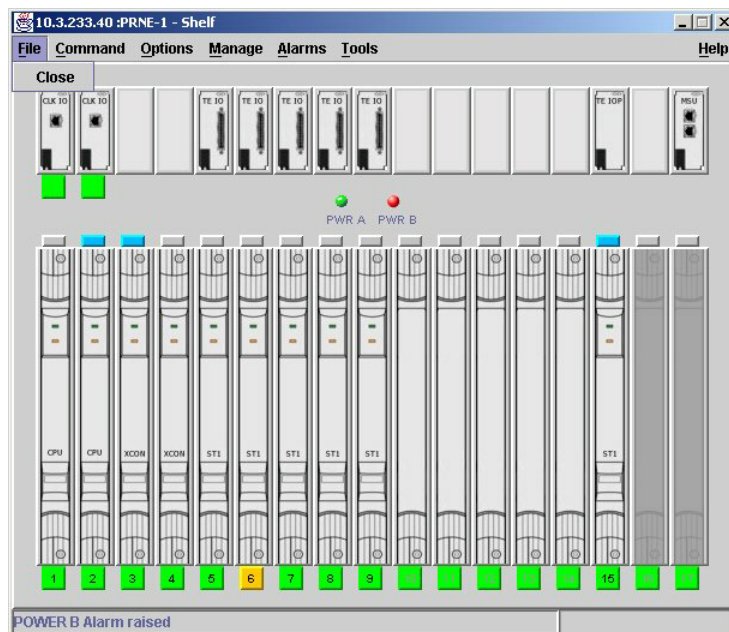
Result: The CMT Console window appears and remains open during the entire CMT session (Figure 5-8). (Ignore any error messages.)

Figure 5-8 CMT Console Window



Result: The CMT main window (Shelf) appears (Figure 5-9).

Figure 5-9 CMT Main Window (Shelf)



4 From the **Options** menu, select **Ethernet**.

Result: The Options dialog box appears.

Procedure 5-4 How to View the ARCA-DACS Configuration (Continued)

5	<p>On the Options dialog box, click the following tabs to view the configuration of the ARCA-DACS:</p> <ul style="list-style-type: none">• Ethernet• Route-Ether• Clock• Node (provides date and time information)• User-Secure (password information)• SNMP• Community Name (used by HP OpenView to identify the ARCA-DACS)• NTP (set NTP time and frequency of the request)• Time-Out
6	<p>Click Close to close the dialog box.</p>

Backing Up and Restoring the ARCA-DACs

This section contains the requirements and procedures to backup or restore the ARCA-DACS configuration.

ARCA-DACS Backup and Restore Requirements

To perform this process, you need the following:

- PC requirements:
 - Windows NT® version 4.0 or higher installed or Windows® 2000, 64 Mb RAM, and 50 MB hard drive space available.
 - Vendor-supplied CMT software for NT, release 2.5.2 installed. (See Procedure 5-5, "How to Install the CMT Software," on page 5-13, for details.)
 - 3Com TFTP server application installed. (See "Installing the 3Com TFTP Server Software" on page 5-7.)
- Vendor-supplied DB9 adapter, connected to the PC COM1 port and the ARCA-DACS CRAFT port (via an RJ45-to-RJ45 cable).
- Ethernet cross-connect cable (RJ45-to-RJ45).
- IP address of the ARCA-DACS and IP address of the PC (any unused IP address on the ARCA-DACS subnet).

Installing the Configuration Management Tool Software



NOTE

You must have administrator privileges to install the CMT software.

Follow Procedure 5-5, "How to Install the CMT Software," on page 5-13.

Procedure 5-5 How to Install the CMT Software

1	Insert the CMT software CD-ROM into the CD-ROM drive.
2	Execute the setup.bat file, which is located in the root directory of the CMT software CD-ROM.
3	Follow the screen prompts while the setup.bat file is running. <div data-bbox="388 781 490 892"></div> <div data-bbox="571 812 685 850" data-label="Section-Header"><h3>NOTE</h3></div> <div data-bbox="505 898 1226 961" data-label="Text"><p>Do not install the software into a directory that contains spaces in the name.</p></div> <div data-bbox="378 976 1258 1071" data-label="Text"><p>Result: The installation utility creates an icon on the Start menu, under Programs, called CMT2.5.2 and installs a CMT2.5.2 shortcut icon on the desktop (Figure 5-10).</p></div> <div data-bbox="378 1106 786 1142" data-label="Caption"><p>Figure 5-10 CMT Shortcut Icon</p></div> <div data-bbox="383 1167 506 1295" data-label="Image"></div>

Backing Up the ARCA-DACS

Procedure 5-6 describes how to back up (upload) the configuration files for the ARCA-DACS.



IMPORTANT

An NVM upload should be performed as soon as possible after upgrading the system, so that your backup copy of configuration data is compatible with the new software.

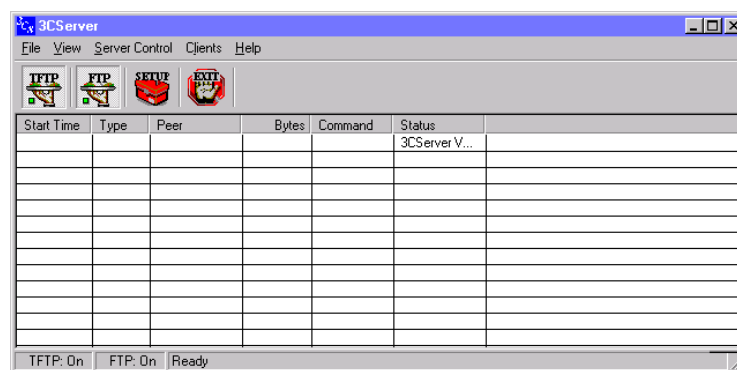
Procedure 5-6 How to Back Up the ARCA-DACS

- 1 Connect the Ethernet port on the PC to the jack labeled 10BT on the Clk IO board of the ARCA-DACS.

- 2 Open the 3CServer TFTP server application.

Result: The 3CServer window appears (Figure 5-11).

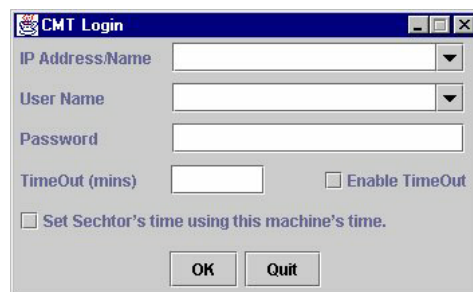
Figure 5-11 3CServer Window



- 3 Double-click the **CMT2.5.2** desktop shortcut icon to open the CMT application.

Result: The CMT Login dialog box appears (Figure 5-12).

Figure 5-12 CMT Login Dialog Box



Procedure 5-6 How to Back Up the ARCA-DACS (Continued)

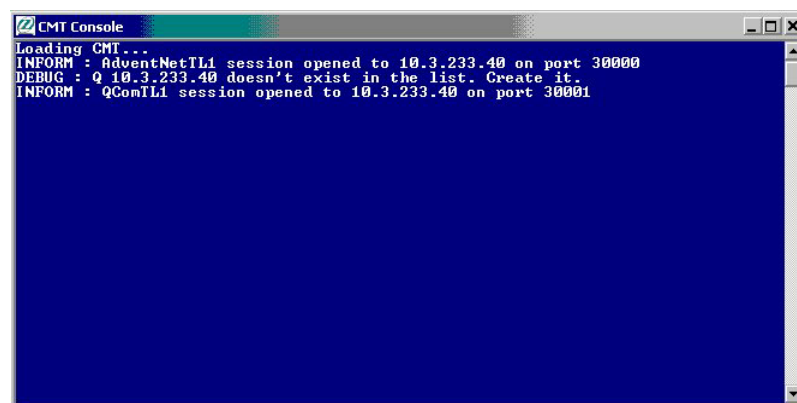
- 4** Do the following to log on:
- 1.** In the **IP Address/Name** box, type the IP address of the ARCA-DACS (using the format **nnn.nnn.nnn.nnn**, where **nnn** = (0-255) (for example, “43.166.199.23”)), and press **Tab**.
 - 2.** In the **User Name** box, type the user name and press Tab. (If the ARCA-DACS is not provisioned, type **ROOT**; it is case-sensitive.)
 - 3.** In the **Password** box, type the password (for root-level access, type the default password, **factory1%**) and press **Tab**.
 - 4.** In the **TimeOut (mins)** box, type the TimeOut time that you want (for example, 30 minutes) and press **Tab**.
 - 5.** Select the **Enable TimeOut** check box.
 - 6.** Do **not** select the Set Sechtor’s time using this machine’s time check box because NTP time setting will not take effect.
-

Procedure 5-6 How to Back Up the ARCA-DACS (Continued)

5 Click **OK**.

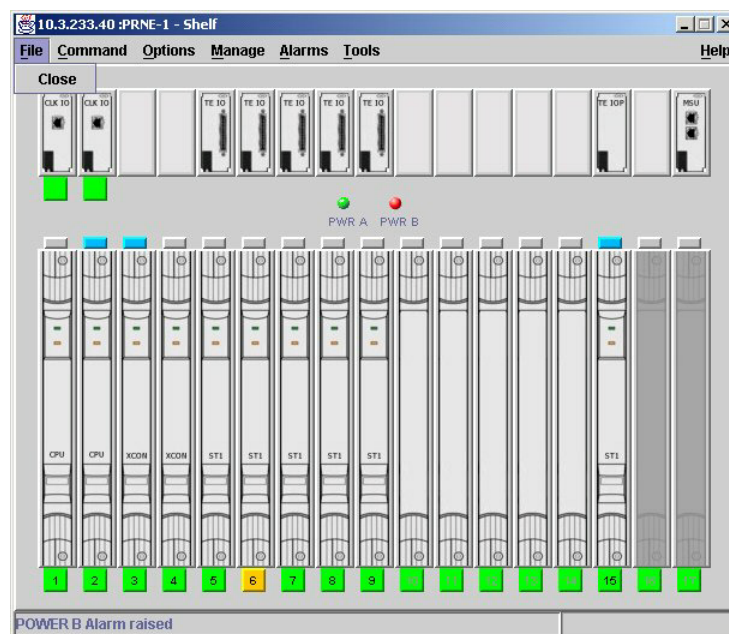
Result: The CMT Console window appears and remains open during the entire CMT session (Figure 5-13). (Ignore any error messages.)

Figure 5-13 CMT Console Window



Result: The CMT main window (Shelf) appears (Figure 5-14).

Figure 5-14 CMT Main Window (Shelf)



6 On the Options menu, click **NVRAM**.

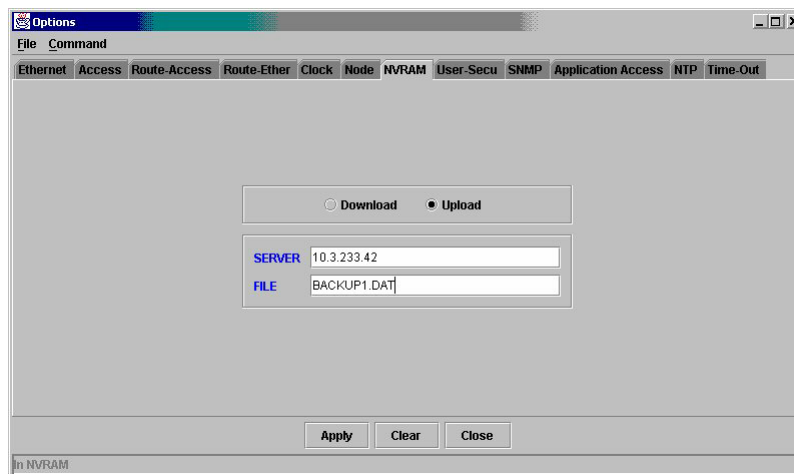
Result: The NVRAM tab appears.

Procedure 5-6 How to Back Up the ARCA-DACS (Continued)

- 7** On the NVRAM tab (Figure 5-15), click the **Upload** radio button.
- In the **SERVER** box, the IP address of your PC is automatically filled-in.
 - In the **FILE** box, type the file name of the backup file. The name must have a .dat extension and no spaces or dashes.

Result: The parameters of the backup are set.

Figure 5-15 NVRAM Tab



Procedure 5-6 How to Back Up the ARCA-DACS (Continued)

8

Click **Apply**.



CAUTION

The Clear command erases all settings and configuration. Do NOT use this option unless you have first uploaded NVRAM and saved the file as a backup. You must restart the CMT after performing this operation.

Result: The configuration begins uploading to the backup1.dat file. You can watch the backup progress in the TFTP window (Figure 5-16).

Figure 5-16 Backup Progress

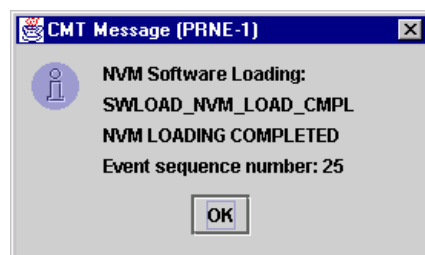
[illegible]

9

When the backup configuration file has finished being created on the PC, a CMT message dialog box appears (Figure 5-17). Click **OK**.

Result: The backup is complete.

Figure 5-17 CMT Message Dialog Box



Restoring the ARCA-DACS

Procedure 5-7 describes how to restore (download) the PC backup configuration files to the ARCA-DACS.



NOTE

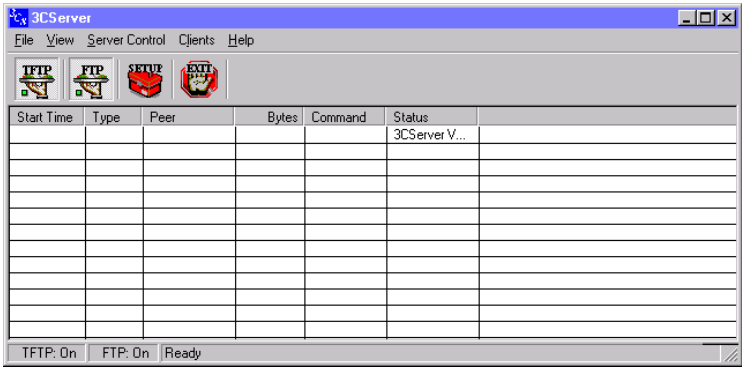
An NVM download takes a significant amount of time.

Procedure 5-7 How to Restore the ARCA-DACS

1 Connect the PC Ethernet port to the jack labeled 10BT on the Clk IO board of the ARCA-DACS.

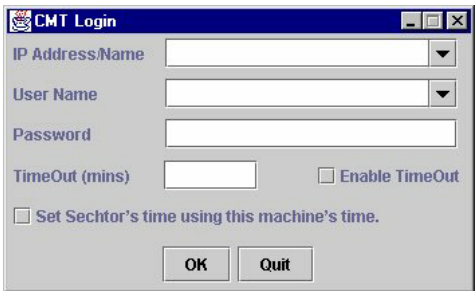
2 Open the 3CServer TFTP server application.
Result: The 3CServer window appears (Figure 5-18).

Figure 5-18 3CServer Window



3 Double-click the **CMT2.5.2** desktop shortcut icon to open the CMT application.
Result: The CMT Login dialog box appears (Figure 5-19).

Figure 5-19 CMT Login Dialog Box



Procedure 5-7 How to Restore the ARCA-DACS (Continued)

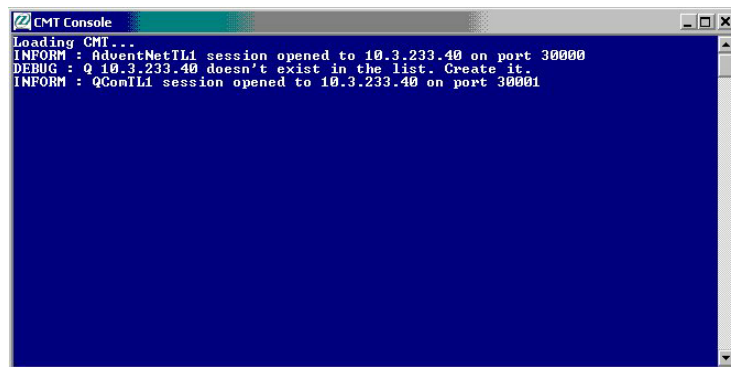
- 4** Do the following to log on:
- 1.** In the **IP Address/Name** box, type the IP address of the ARCA-DACS (using the format **nnn.nnn.nnn.nnn**, where **nnn** = (0-255) (for example, “43.166.199.23”)), and press **Tab**.
 - 2.** In the **User Name** box, type the user name and press Tab. (If the ARCA-DACS is not provisioned, type **ROOT**; it is case-sensitive.)
 - 3.** In the **Password** box, type the password (for root-level access, type the default password, **factory1%**) and press **Tab**.
 - 4.** In the **TimeOut (mins)** box, type the TimeOut time that you want (for example, 30 minutes) and press **Tab**.
 - 5.** Select the **Enable TimeOut** check box.
 - 6.** Do **not** select the Set Sector’s time using this machine’s time check box because NTP time setting will not take effect.
-

Procedure 5-7 How to Restore the ARCA-DACS (Continued)

5 Click **OK**.

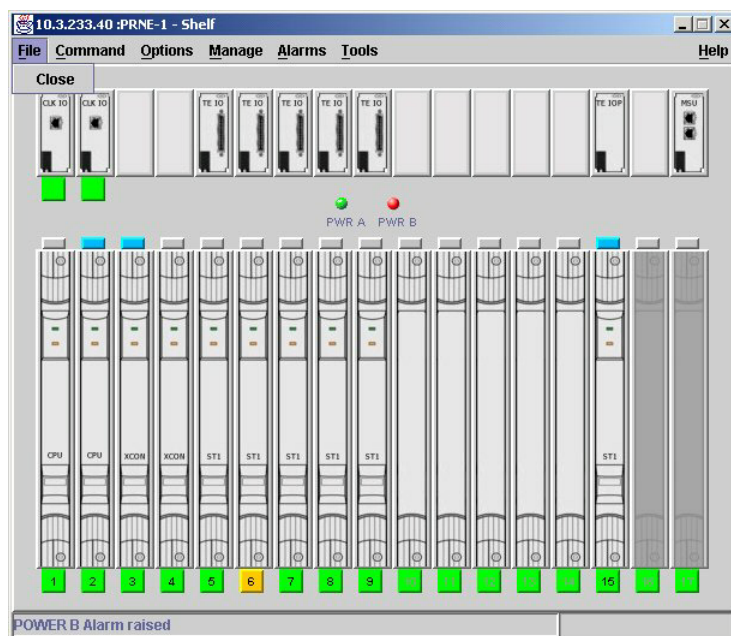
Result: The CMT Console window appears and remains open during the entire CMT session (Figure 5-20). (Ignore any error messages.)

Figure 5-20 CMT Console Window



Result: The Shelf window appears (Figure 5-21).

Figure 5-21 Shelf Window

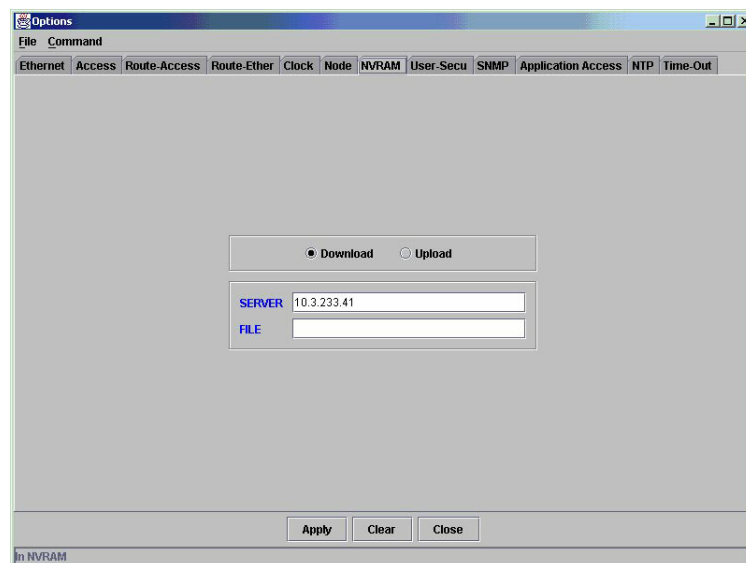


Procedure 5-7 How to Restore the ARCA-DACS (Continued)

6 On the Options menu, select **NVRAM**.

Result: The NVRAM tab appears (Figure 5-22).

Figure 5-22 NVRAM Tab



7 On the NVRAM tab, click the **Download** radio button.

- In the **SERVER** box, the IP address of your PC is automatically filled-in.
- In the **FILE** box, type the file name of the backup file created from the configuration data that was previously uploaded to the PC. You must match the name of the file that was uploaded to the PC exactly.

Result: The parameters of the restore are set.

Procedure 5-7 How to Restore the ARCA-DACS (Continued)

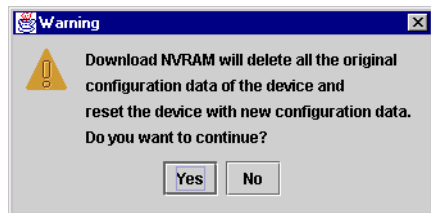
8 Click **Apply**.

**CAUTION**

The Clear command erases all settings and configuration. Do NOT use this option unless you have first uploaded NVRAM and saved the file as a backup. You must restart the CMT after performing this operation.

Result: A verification CMT message appears (Figure 5-23).

Figure 5-23 Warning Dialog Box



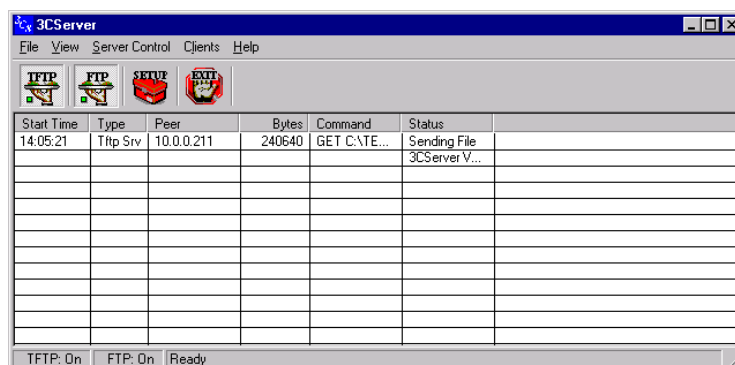
9 Click **Yes** to dismiss the warning.

Result: The configuration begins downloading to the ARCA-DACS.

Procedure 5-7 How to Restore the ARCA-DACS (Continued)

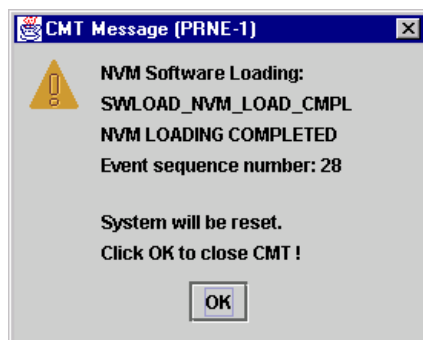
- 10** Watch the restore progress in the 3CServer window (Figure 5-24).

Figure 5-24 Restore Progress



- 11** When the restoration is complete, a CMT message appears (Figure 5-25). Click **OK**.

Figure 5-25 CMT Message Dialog Box



Result: The download is complete. The ARCA-DACS resets and the CMT application closes.

Managing the Channel Bank

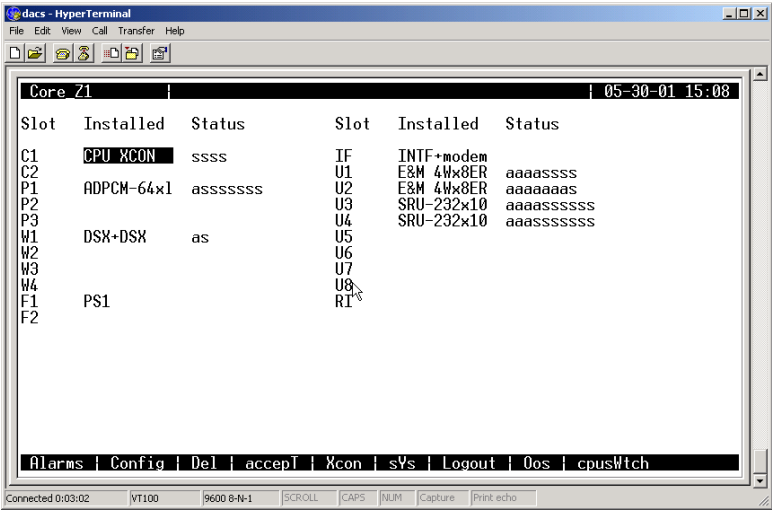
This section describes how to view the configuration of the channel bank, then how to back up or restore the data. “Channel bank” refers to the Telecommunications Network Server (TeNSr).

See Volume 9, *Master Site Hardware and Software Configuration* for configuration information.

Viewing the Channel Bank Configuration

Procedure 5-8 describes how to view the channel bank configuration. This procedure assumes the channel bank software version is 5.3.1.

Procedure 5-8 How to View the Channel Bank Configuration

1	Connect the serial cable from the PC COM1 port to the TERM port on the interface board in the channel bank. (The port settings are 9600 8-N-1, none.)
2	Open Microsoft HyperTerminal and press Enter twice. Result: The PC establishes a serial connection to the channel bank.
3	At the password prompt, type the manager password, and press Enter . Result: The channel bank main screen appears (Figure 5-26).
Figure 5-26 Channel Bank Main Screen	
 The screenshot shows a HyperTerminal window titled 'dacs - HyperTerminal'. The main display area shows the 'Core Z1' screen with a timestamp '05-30-01 15:08'. It contains a table with columns 'Slot', 'Installed', and 'Status'. The table lists various components like CPU XCON, ADPCM-64x1, DSX+DSX, PS1, IF, INTF+modem, and several E&M and SRU modules. At the bottom, there is a menu bar with options: Alarms, Config, Del, accept, Xcon, sVs, Logout, Oos, and cpusWtch. The status bar at the very bottom shows connection details: 'Connected 0:03:02', 'VT100', '9600 8-N-1', and various control options like SCROLL, CAPS, NUM, Capture, and Print echo.	
4	Press the up or down arrows on the key board to select a card to view the configuration. Press Enter to select the card.
5	View the configuration for the card and then return to the main menu.

Backing Up and Restoring the Channel Bank

This section contains the requirements and procedures to back up or restore the channel bank configuration.

Channel Bank Backup and Restore Requirements

To perform this procedure, you need the following:

- PC with Microsoft HyperTerminal installed. (See "Setting Up Microsoft HyperTerminal Software" on page 5-3 for details.)

- Serial cable female DB9-to-RJ45 flat cable with DB9 adapter or female DB9.

Backing Up the Channel Bank

Procedure 5-9 allows you to save the configuration parameters for the following:

- All cards or individual cards
- The installation table
- Cross-connects
- Alarm filters
- Alarm history

This information can then be used to restore the parameter data to certain cards or to the whole system. See "Restoring the Digital Service Unit/Channel Service Unit" on page 5-33.



IMPORTANT

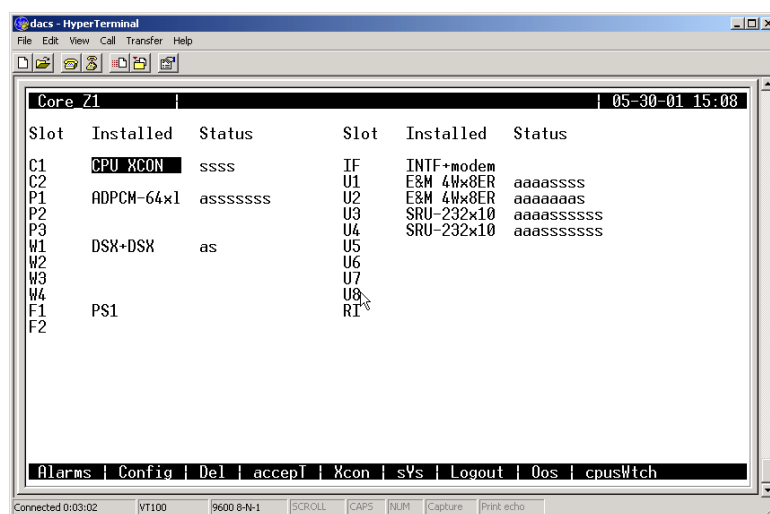
You should back up the system after initially configuring it, and each time you change the channel bank's configuration.

This procedure assumes the channel bank software version is 5.3.1.

Procedure 5-9 How to Back Up the Channel Bank

1	Connect the serial cable from the PC COM1 port to the TERM port on the interface board in the channel bank. (The port settings are 9600 8-N-1, none.)
2	Open Microsoft HyperTerminal and press Enter twice. Result: The PC establishes a serial connection to the channel bank.
3	At the password prompt, type the manager password, and press Enter . Result: The channel bank main screen appears (Figure 5-27).

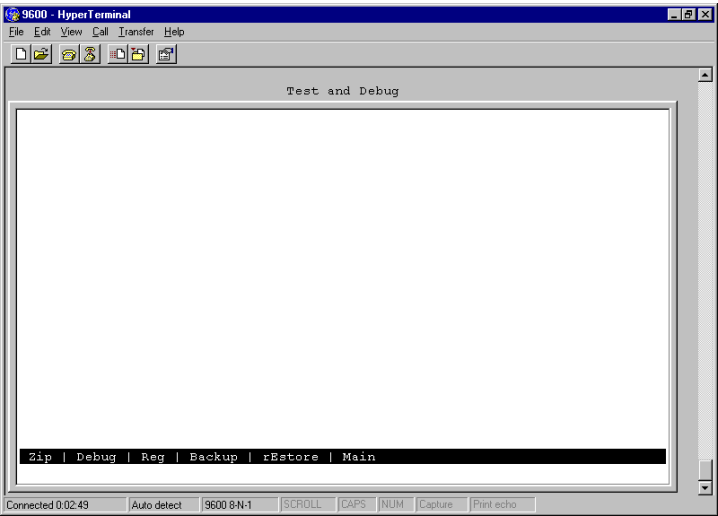
Figure 5-27 Channel Bank Main Screen



Procedure 5-9 How to Back Up the Channel Bank (Continued)

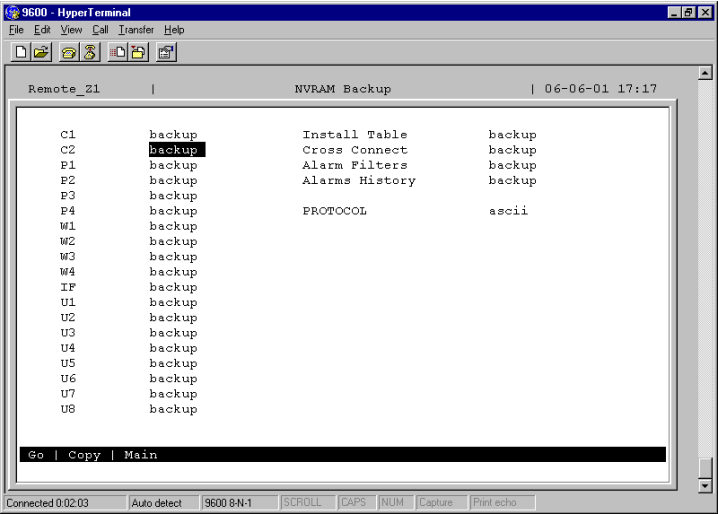
- 4
- On the main screen menu, press **Y** for the sYs (system) option.
Result: The Test and Debug screen appears (Figure 5-28).

Figure 5-28 Test and Debug Screen



- 5
- On the Test and Debug screen menu, press **B** for the Backup option.
Result: The NVRAM Backup screen appears (Figure 5-29).

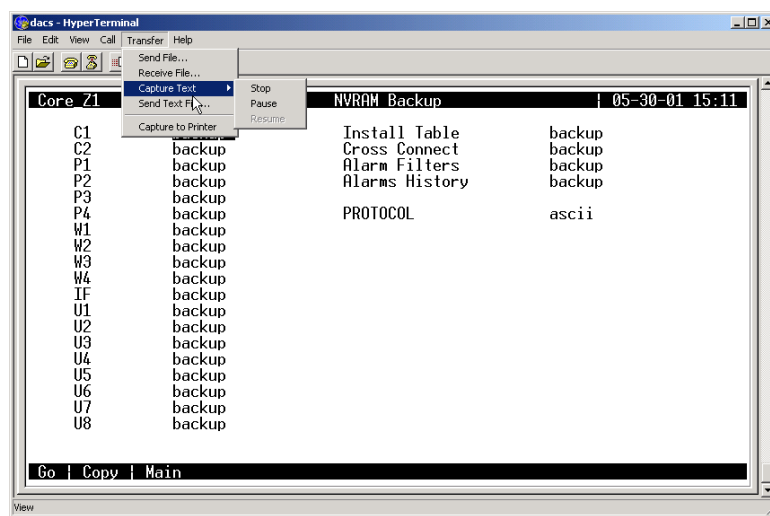
Figure 5-29 NVRAM Backup Screen



- 6
- Ensure the Protocol field is set to **ascii**. If it is not, use the up and down arrow keys to navigate the cursor, highlight the Protocol field, use the left arrow key to toggle the field, and press **Enter**.
Result: The backup protocol is set to **ascii**.

Procedure 5-9 How to Back Up the Channel Bank (Continued)

7	(Optional) Set Microsoft HyperTerminal to XMODEM , if necessary. Result: The backup data can be transferred to the PC.	
8	IF you want:	THEN:
	To do a partial backup:	1. Go to step 9.
	To do a full backup:	1. Go to step 10.
9	Select either backup or no for each channel bank slot. The default information field for each slot is backup . To change any slot to no (which means that no information from that slot will be saved) use the left arrow key to select no , and press Enter . Result: The slot is not backed up. To change a group of consecutive slots to backup or no , highlight the slots that you want to copy and press C (for copy). You can repeat this process to change as many slots as needed.	
10	From the Transfer menu, select Capture Text . Result: The system prompts you for a backup filename, and a path to store the backup file. The filename must include .txt as the extension or the backup will not function properly.	
11	Type the filename and press Enter ; then click Start to start the backup.	
12	On the NVRAM Backup screen menu, press G . Result: The channel back starts transferring the configuration data to a file. This is demonstrated by the screen filling up with scrolling text. When the backup is finished, the text stops scrolling and the message BACKUP COMPLETE displays.	
13	From the Transfers menu, select Capture Text , and then select Stop . Result: The PC stops waiting for the channel bank to send data (Figure 5-30).	

Figure 5-30 Capture Text Menu

Procedure 5-9 How to Back Up the Channel Bank (Continued)

14	On the NVRAM Backup screen menu, press M to return to the main menu. Result: The backup is finished.
15	From the File menu, select Exit to log out. Result: The terminal session closes.
16	Browse to the file location and open the .txt file to confirm the backup.

Restoring the Channel Bank

Procedure 5-10 allows you to restore configuration parameters for:

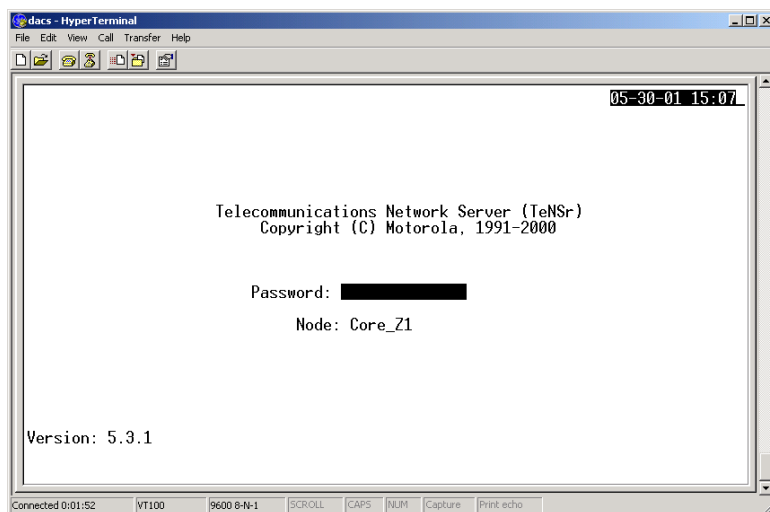
- All or some cards
- Installation table
- Cross-connects
- Alarm filters

This procedure assumes the channel bank software version is 5.3.1.

Procedure 5-10 How to Restore the Channel Bank

1	Connect the serial cable from the PC COM1 port to the TERM port on the interface board in the channel bank. (The port settings are 9600 8-N-1, none.)
2	Open Microsoft HyperTerminal and press Enter twice. Result: The PC establishes a serial connection to the channel bank and the logon screen appears (Figure 5-31).

Figure 5-31 Channel Bank Login Screen

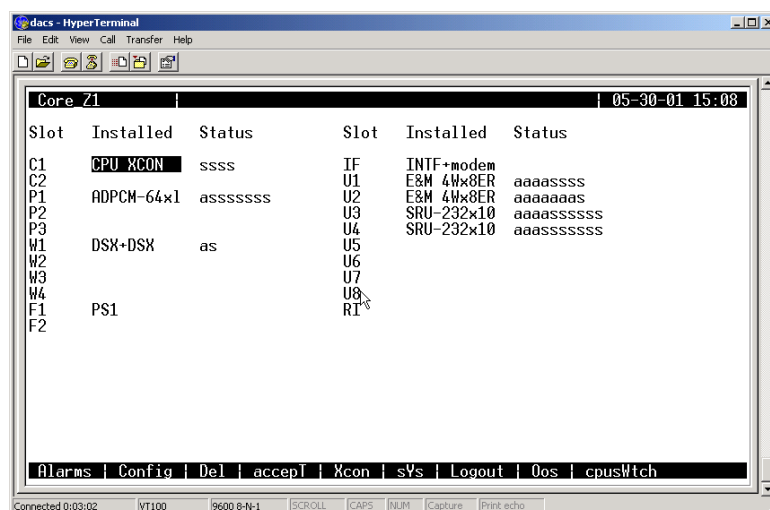


Procedure 5-10 How to Restore the Channel Bank (Continued)

- 3** At the password prompt, type the manager password, and press **Enter**.

Result: The channel bank main screen appears (Figure 5-32).

Figure 5-32 Channel Bank Main Screen



- 4** On the main screen menu, press **Y** for sYs (system).

Result: The Test and Debug screen appears.

- 5** On the Test and Debug screen menu, press **E** for rEstore.

Result: The Restore screen appears.

- 6** Ensure the **Protocol** field is set to **ascii**. If it is not, use the up and down arrow keys to navigate the cursor, highlight the **Protocol** field, use the left arrow key to toggle the field, and press **Enter**.

Result: The restore protocol is set to ascii.

- 7** **IF you want:** **THEN:**

To do a partial restore:

1. Go to step 8.


To do a full restore:

1. Go to step 9.

- 8** Select either **restore** or **no** for each channel bank slot. The default information field for each slot is **restore**. To change any slot to **no**, which means that information from that slot will not be restored, use the left arrow key to highlight **no**, and press **Enter**.

Result: The slot is not restored. To change a group of consecutive slots to **restore** or **no**, highlight the slots that you want to copy and press **C** (for copy). You can repeat this process to change as many slots as needed.

Procedure 5-10 How to Restore the Channel Bank (Continued)

9	<p>From the Restore screen menu, press G.</p> <p>Result: The following message displays:</p> <p>Restore is active</p>
10	<p>From the Transfers menu, select Send Text File. The system prompts you for a backup file filename, and a path to retrieve the backup file. Type the filename, and press Enter.</p> <p>Result: The restore process begins. A message appears when it is complete.</p> <div><div></div><div><div>NOTE</div><p>If a process completed message appears immediately following the start of the process, an error has occurred. If this happens, check to ensure that the file being sent to the channel bank has a .txt extension, and Capture Text is stopped.</p></div></div>
11	<p>When the channel bank restoration is complete, press Esc twice to reboot.</p> <p>Result: The channel bank reboots itself.</p>
12	<p>When the channel bank has rebooted, press Y when prompted.</p> <p>Result: The channel bank configuration information is restored.</p>

Managing the Digital Service Unit/Channel Service Unit



This section describes how to view the configuration of the Digital Service Unit (DSU)/Channel Service Unit (CSU), then how to back up or restore the data. DSU/CSUs are an optional device that is used for connectivity to remote Network Management clients.

Viewing the Digital Service Unit/Channel Service Unit Configuration

You can view the DSU/CSU configuration by referring to the paper copies of the settings entered into the DSU/CSU from the Line Parameters screen. You can also use the key pad to scroll through the settings. The following list shows the keys that can be used to navigate through the menus:

- Press the **Enter** key to select active menu items or save manually entered information.
- Press the number of the item to select a menu item.

- Press the **Cancel** key to stop the current activity and return to the previous menu. Repeat until the desired menu level is reached.
- Press the **Up and Down arrows** to scroll through the sub-items menu available in the current menu.

Backing Up and Restoring the Digital Service Unit/Channel Service Unit

This section contains the guidelines to backup or restore the DSU/CSU configuration.

Backing Up the Digital Service Unit/Channel Service Unit

The DSU/CSU configuration data backup consists of writing down the settings entered into the DSU/CSU from the Line Parameters screen and keeping paper copies in a safe place.



IMPORTANT

Each DSU/CSU has a unique set of line parameter values and each set needs to be identified accordingly.

Restoring the Digital Service Unit/Channel Service Unit

The restoration of DSU/CSU configuration data consists of re-entering line parameter settings into the DSU/CSU from the Line Parameters screen.



IMPORTANT

The written line parameters must be specifically for the DSU/CSU being restored.

Managing the HP Procurve Ethernet Switch



This section describes how to view the configuration of the HP® Procurve® 2524 Ethernet switch then how to back up or restore the data.

This section does **not** discuss how to configure the switch. See Volume 9, *Master Site Hardware and Software Configuration* for configuration procedures.

Viewing the Ethernet Switch Configuration

Procedure 5-11 describes how to view the Ethernet switch configuration.

Procedure 5-11 How to View the Ethernet Switch Configuration

1	Connect a serial cable from the PC COM1 port to the CONSOLE port on the front of the switch.
2	Connect the PC Ethernet port to the switch.
3	Open Microsoft HyperTerminal and press Enter twice. Result: The PC establishes a serial connection to the switch.
4	At the login prompt, type the user name, and press Enter , then type the manager password, and press Enter .



NOTE

Ethernet switches that are not configured have no password, so just press **Enter**.

Result: The console main menu appears (Figure 5-33). (If it does not appear, type **menu** and press **Enter**.)

Figure 5-33 Console Main Menu

```

4.1test-1
===== CONSOLE - MANAGER MODE =====
Main Menu

1. Status and Counters...
2. Switch Configuration...
3. Console Passwords...
4. Event Log
5. Command Line (CLI)
6. Reboot Switch
7. Download OS
8. Run Setup
9. Stacking...
0. Logout

Provides the menu to display configuration, status, and counters.
To select menu item, press item number, or highlight item and press <Enter>.

```

Procedure 5-11 How to View the Ethernet Switch Configuration (Continued)

5	Press 2 , Switch Configuration, and press Enter . Result: The Switch Configuration menu appears.
6	From the Switch Configuration menu, you can view the following configuration information: <ul style="list-style-type: none">• Port/trunk settings• Network monitoring port• IP configuration• SNMP communities

Backing Up and Restoring the Ethernet Switch

This section contains the procedures to back up or restore the configuration file of the Ethernet switch.

Ethernet Switch Backup and Restore Requirements

To perform this procedure, you need the following:

- PC with Microsoft HyperTerminal installed. (See "Setting Up Microsoft HyperTerminal Software" on page 5-3.)
- Serial cable (female DB9-to-female DB9).
- Ethernet-capable PC with the 3Com TFTP server application installed. (See "Installing the 3Com TFTP Server Software" on page 5-7 for details.)
- Ethernet cable.
- IP address of the Ethernet switch and the PC.
To find or set the PC IP address, click **Start**, and then select **Settings**, and select **Control Panel**. Double-click the Network icon and select the **Protocols** tab.

**IMPORTANT**

The PC IP address must be set to an available IP address on the subnet.

Backing Up the Ethernet Switch

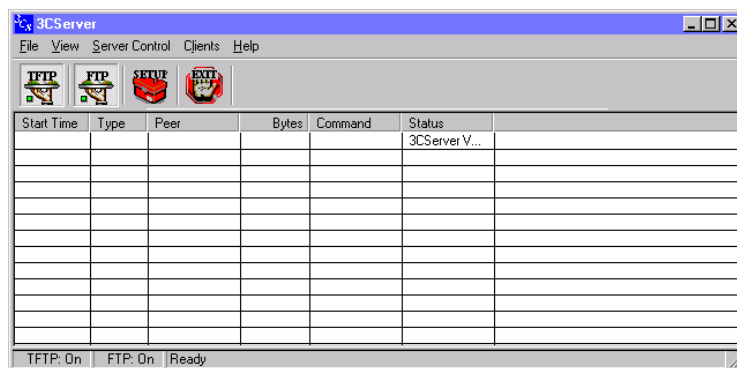
Procedure 5-12 describes how to back up configuration information for the HP J2524 Ethernet switch.

Procedure 5-12 How to Back Up the Ethernet Switch

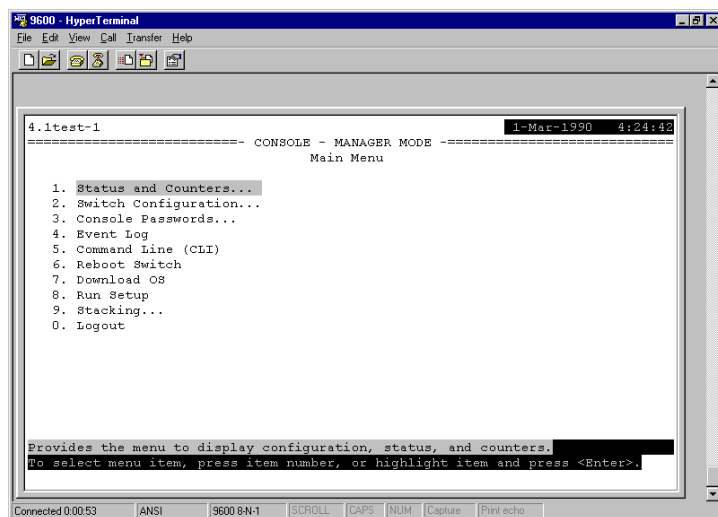
1	Connect a serial cable from the PC COM1 port to the CONSOLE port on the front of the switch.
2	Connect the PC Ethernet port to the switch.

Procedure 5-12 How to Back Up the Ethernet Switch (Continued)

- 3** Open the 3CServer TFTP server application.
Result: The 3CServer window appears (Figure 5-34).

Figure 5-34 3CServer Window

- 4** Open Microsoft HyperTerminal and press **Enter** twice.
Result: The PC establishes a serial connection to the switch.
- 5** At the login prompt, type the user name, and press **Enter**, then type the manager password, and press **Enter**.
 Ethernet switches that are not configured have no password, so just press **Enter**.
Result: The console main menu appears (Figure 5-35).

Figure 5-35 Console Main Menu

Procedure 5-12 How to Back Up the Ethernet Switch (Continued)

6	From the main menu, select 5. Command Line (CLI) . Result: HP2524# becomes the CLI prompt.
7	Type the following command which includes the PC IP address: copy startup-config tftp 10.1.1.200 Switch1 Result: The startup-config file of the switch copies to the server IP address, and names the stored file Switch1 . The Switch1 file is stored in the directory set up using the TFTP server application.

Restoring the Ethernet Switch

Follow Procedure 5-13 to restore the Ethernet switch.

Procedure 5-13 How to Restore the Ethernet Switch

1	Connect a serial cable from the PC COM1 port to the CONSOLE port on the front of the switch.
2	Connect the PC Ethernet port to the switch.
3	Ensure the TFTP server application is open. Result: The PC establishes a LAN connection to the switch.
4	Open Microsoft HyperTerminal and press Enter twice. Result: The PC establishes a serial connection to the switch and the HP2524# prompt appears.
5	Type Setup and enter the following switch information: <ul style="list-style-type: none"> • Default gateway • IP address • Network Mask Result: The switch can be recognized by other devices on the LAN.
6	Type Save to save the configuration. Result: The configuration is saved.
7	Highlight Cancel and press Enter . Result: The HP2524# prompt is displayed.
8	Type the following command: copy tftp startup-config 10.2.104.222 Switch1 Result: The Switch1 file is copied from the TFTP server (PC IP address 10.2.104.222) to the Ethernet switch, and renames the file startup-config . Once the startup-config file is received by the Ethernet switch, it reboots and runs the new startup-config file.

Managing the Modem

This section describes how to view the configuration of the modem, then how to back up or restore the data.

For connectivity to the modem and configuration information, see Volume 9, *Master Site Hardware and Software Configuration*.

Viewing the Modem Configuration

Procedure 5-14 describes how to view the modem configuration using the modem key pad to scroll through the modem settings. Select each category in the modem and go through each setting to get the current setup.



NOTE

Your system may use various models of the modem, so this procedure should only be used as a guideline. See the **Paradyne** documentation for your model for more information about using the modem.



NOTE

F_ is used to indicate the function key (**F1**, **F2**, or **F3**) that is directly under the option that you want to select.

Procedure 5-14 How to View the Modem Configuration

1	Press Scroll Forward (>) , the right arrow button located on the front panel of the modem, several times until the Configure option appears. Result: The Configure option appears on the LED screen.
2	Press the F_ key under the Configure option to select it, where F_ is the key directly under the Configure option. The option depends on which side of the LED screen Configure appears. Result: The Configure Option is selected.
3	Press F1 to select the Activ (Operating) option. Result: The Activ (Operating) option is selected.
4	Press F1 to select the Edit option. Result: The Edit option is selected.
5	Press F1 to select Edit .
6	Press F1 to select DTE Interface . Result: The Configure Option appears in the LED screen.
7	Press F1 to select Next and begin to view the settings for DTE Interface. Result: The first setting appears.
8	View the parameters in order selecting Next to continue to the next setting. At the end of Each Strap group, an END option will display.
9	Press F1 to select the END option, and then scroll to the next parameter group using the Scroll Forward (>) right arrow.
10	Access the next menu, DTE Dialer , and continue through the options for that menu and subsequent menus, viewing the settings.



NOTE

See Volume 9, *Master Site Hardware and Software Configuration* for a list of settings.

Backing Up and Restoring the Modem

This section contains the procedures to backup or restore the modem configuration.

Backing Up the Modem

The modem backup simply consists of writing down the modem settings. You can view the settings using Procedure 5-14 or see Volume 9, *Master Site Hardware and Software Configuration* for the procedures and settings. Keep the paper in a safe place in case the settings need to be reloaded.

Restoring the Modem

The procedure for restoring the modem simply consists of re-entering the modem settings that were written down on paper for the backup.

Managing the TRAK 9100

This section describes how to view the configuration of the TRAK 9100 and includes the backup and restore procedures.

See Volume 9, *Master Site Hardware and Software Configuration* for installation information.

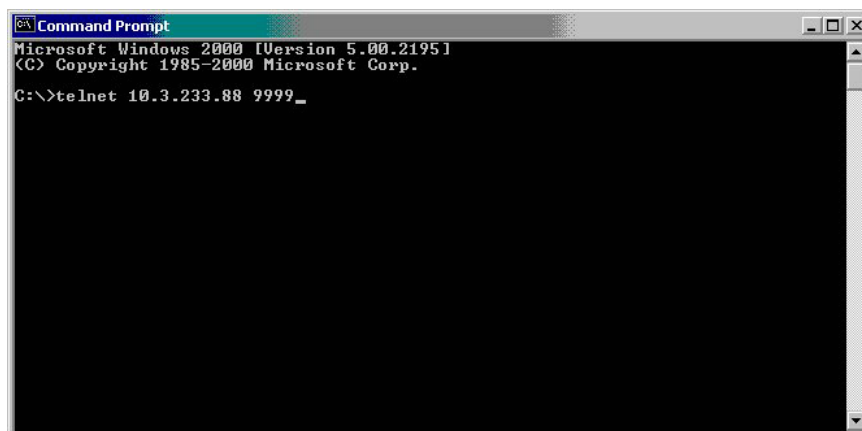
Viewing the TRAK 9100 Configuration

Procedure 5-15 describes how to telnet into the port to view the configuration. All settings on the user cards are done through jumper switches.

Procedure 5-15 How to View the TRAK 9100 Configuration

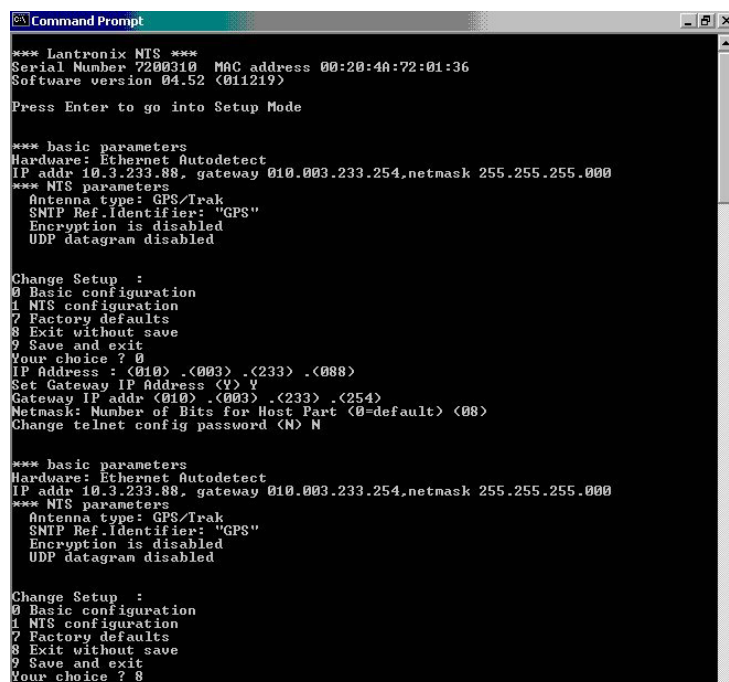
- 1 Telnet to the TRAK 9100 port, 9999 (Figure 5-36).

Figure 5-36 Telnet Screen



- 2 Press **Enter** to access setup mode. You can view the IP address, Gateway IP address, and Netmask (Figure 5-37).

Figure 5-37 Setup Mode Screen



Backing Up and Restoring the TRAK 9100

You cannot back up or restore the TRAK 9100 configuration. The configuration is stored in nonvolatile memory, so even after a power cycle, you can view the configuration.

If the configuration is lost, you must re-enter the configuration.

Index

3Com TFTP Server	
main window	5-36
software installation	5-7
using to back up the Ethernet switch.	5-35

A

accessing		procedure	3-10
a device using the terminal server	4-10	adding switches	
CiscoView.	1-11	LAN switch images to library.	1-52
CiscoWorks2000.	1-5	WAN switch.	2-23
Component Information Viewer.	2-41	ARCA-DACS	
MDMWeb.	2-49	backup	5-14
Preside MDM	2-4	CMT software installation	5-14
remote terminal server	4-6	restore.	5-19
Resource Manager Essentials	1-36	ASAP radio button (Reboot display)	
terminal server.	4-8	immediate reboot	3-26
Add Router display.	3-11	verifying software upgrade	3-43
adding routers		At radio button (Reboot display).	3-30
preparation	3-9		

B

backing up		configuring	3-10
ARCA-DACS	5-14	setting.	3-32
channel bank	5-27	Boot Directory (Reboot display)	
DSU/CSU	5-33	after specified interval	3-28
Ethernet switch	5-35	at specified time	3-30
files on the FullVision INM server	3-21	immediate reboot	3-26
LAN switch configuration	1-42	rebooting routers to update portal	3-53
LAN switch software.	1-42	verify the software upgrade	3-43
modem	5-40	Boot Directory (View Router display)	3-34
terminal server.	4-20	boot.cfg file	3-10
three-copy backup rule	5-2	adding with router	3-11
TRAK 9100	5-42	capturing from routers	3-17
WAN switch data	2-14	checksumming.	3-39
Backup display.	3-22	downloading to routers	3-14
Backup/Export Configuration Files Only radio button		uploading from router	3-11
(Backup display)	3-22	viewing	3-37
BCUB file format	3-54	Both Primary and Secondary radio button (Perform	
boot blocks		Checksum display)	3-38

C

- Cancel All Jobs (Action menu option) 3-40
- Cancel My Jobs (Action menu option) 3-40
- Cancel Reboot button (Reboot display)
 - restriction 3-27
 - scheduled reboots 3-32
- canceling jobs 3-39
- canceling scheduled reboots 3-32
- Capture display 3-17
- capture.cfg file
 - capturing from routers 3-17
 - viewing 3-37
- capturing files from routers
 - overview 3-16
 - procedure 3-17
- card, resetting on WAN switch 2-45
- Catalyst image files
 - copying to server. 1-50
 - copying to TNM client 1-50
- channel bank
 - backup 5-27
 - backup and restore requirements 5-26
 - restore. 5-30
 - viewing the configuration. 5-26
- checking device configuration changes
 - Startup vs. Running example 1-63
 - two versions of same device example 1-59
- Checksum button (View Router display) 3-36
- checksums
 - comparing to FullVision INM server 3-39
 - performing 3-36
 - procedure 3-37
- Choose Reboot Time dialog box 3-31
- Choose Time button (Reboot display) 3-31
- CiscoView
 - accessing 1-11
 - creating system logs 1-23
 - displaying VLAN members. 1-17
 - fault management 1-33
 - features 1-9
 - LAN switch performance 1-27
 - monitoring Ethernet port performance 1-19
 - monitoring LAN switch performance 1-27
 - monitoring MSFC routers. 1-31
 - monitoring system logs 1-26
 - MSFC routers, monitoring 1-31
 - resetting Ethernet module. 1-33
 - system logs
 - creating 1-23
 - monitoring 1-26
 - using 1-9
 - viewing system information. 1-14
 - viewing system time 1-15
- CiscoWorks2000
 - accessing 1-5
 - alarms, displaying 1-66
 - displaying alarms 1-66
 - exiting 1-9
 - managing security access 1-2
 - security access 1-2
- CMT
 - setup 5-14
- collecting performance information 2-34
- colors
 - showing status for LAN switch components 1-10
 - showing status for WAN switch components 2-38
- command keys, terminal server 4-5
- command line
 - backing up the Ethernet switch 5-37
 - Command Console user interface 2-29
 - connecting to the WAN switch, MDMWeb. 2-53
 - using to connect to WAN switch, client 2-30
- command log, router
 - capturing from routers 3-17
 - checksumming. 3-39
 - viewing 3-37
- Commit TestBoot button (Reboot display)
 - cancel the watchdog timer 3-27
 - verifying software upgrade 3-44
- community strings
 - assigning to router 3-10
- Compare to Server (Perform Checksum display) 3-39
- Component (Session/Full Log column). 3-19
- Component Information Viewer
 - accessing 2-41
 - collecting faults on the WAN switch. 2-41
- configuration
 - data management 5-1
 - restoring LAN switch 1-42
 - viewing router configuration 3-59
 - viewing the channel bank configuration 5-26
 - viewing the Ethernet switch configuration 5-34
 - viewing the LAN switch configuration. 1-39
 - viewing the modem configuration 5-38
 - viewing the terminal server configuration 4-19
 - viewing the TRAK 9100 configuration 5-41
- configuration applications, launching 3-33
- configuration data backup guidelines
 - data management 5-2
- configuration file 3-10
 - adding with router 3-11

capturing from routers	3-17	Configuration File check box (Perform Checksum display)	3-39
checksumming.	3-39	connecting to WAN switch	
downloading to routers	3-14	command line from client workstation	2-30
uploading from router	3-11	command line using MDMWeb	2-53
viewing	3-37	copying Catalyst image files	
Configuration File check box (Capture display)	3-18	to ESMS server	1-50
Configuration File check box (Download display)		to TNM client	1-50
downloading files from the server	3-16	creating system logs	1-23

D

data flow between PC, FullVision INM server, and routers.	3-14	download EOS software to secondary directory	3-45
Date (Session/Full Log column).	3-19	download new EOS software to primary directory	3-42
Default radio button (Reboot display)		figure	3-15
after a specified interval	3-28	Download software pull-down list (Download display)	
at specified time	3-30	downloading EOS software to primary boot directory	3-42
immediate reboot	3-26	Download Software pull-down list (Download display)	
Delete Router button (View Router display)	3-36	downloading boot image to primary boot directory	3-52
deleting routers		downloading boot image to secondary boot directory	3-51
from the View Router display	3-34	downloading EOS software to secondary boot directory	3-45
option on the View Router display.	3-36	downloading files from the server	3-16
preparation	3-9	Download Specific Files (Download display)	
procedure	3-12	downloading boot image to primary boot directory	3-52
Description (Session/Full Log column).	3-19	downloading boot image to secondary boot directory	3-51
device configuration changes		downloading EOS software to primary boot directory	3-42
checking		downloading EOS software to secondary boot directory	3-45
Startup vs. Running example	1-63	downloading files from the server	3-16
two versions of same device example	1-59	downloading files to routers	
verifying who made	1-65	overview	3-14
device status		procedure	3-15
FullVision INM server backend	3-18	downloading software	
LAN switch	1-10	to the LAN switch	1-49
WAN switch.	2-38	to the WAN switch	2-18
dialing in to terminal server	4-7	DSU/CSU	
displaying alarms		backup	5-33
MDMWeb.	2-55	restore.	5-33
Preside MDM	2-42		
displaying performance information	2-34		
distributing software images to LAN switch or MSFC routers.	1-54		
Download display			
download boot image to primary boot directory	3-52		
download boot image to secondary boot directory	3-51		

E

Enterprise OS Software Reference Guide	3-3	EOS SW check box (Perform Checksum display)	3-39
Enterprise OS Software User Guide	3-2	EOS SW files	
EOS software		checksumming	3-39
recommended procedure for field upgrade	3-40	downloading to routers	3-14
upgrading with portal		Ethernet module, resetting	1-33
overview	3-45	Ethernet port, monitoring performance	
procedure	3-46	Ethernet port performance	1-19
EOS SW check box (Download display)		Ethernet switch	
downloading all software from the server	3-16	backup	5-35
downloading boot image to primary boot		backup and restore requirements	5-35
directory	3-52	restore	5-37
downloading boot image to secondary boot		viewing the configuration	5-34
directory	3-51	exiting CiscoWorks2000	1-9
downloading EOS software to primary boot			
directory	3-42		
downloading EOS software to secondary boot			
directory	3-45		

F

fault management with CiscoView	1-33	using to upgrade EOS firmware	3-49
features, Router Manager UI	3-1	using to upgrade EOS software overview	3-45
Files to Checksum (Perform Checksum display)	3-39	using to upgrade EUS software procedure	3-46
firmware		Full Backup radio button (Backup display)	3-22
upgrade issues	3-47	Full Log display	3-18
upgrading using portal	3-49	viewing	3-19
firmware/software portal		FullVision INM server	
overview	3-48	backing up files on	3-21
		restoring files to	3-23

G

groups	
management tasks for	3-2
managing	3-7
pseudo, procedure	3-10
zAllRouters, procedure	3-10

H

history files, viewing	3-37	managing	5-33
HP OpenView		HyperTerminal	
displaying LAN switch alarms	1-66	channel bank backup and restore	5-26
displaying WAN switch alarms	2-43	Ethernet switch backup and restore	5-35
HP Procurve Switch		setup	5-3

I

images, adding to library	1-52	inventory, performing on WAN switch	2-9
installation of software images	1-58	IP address, assigning to router	3-9

L

LAN switch		library	
backing up the software and configuration . . .	1-42	adding new LAN switch images to	1-52
viewing the configuration.	1-39	logging on	
LAN switch status, monitoring	1-27	CiscoWorks2000.	1-7
Last Accessed (View Router display)	3-34	MDMWeb.	2-50
Last Reboot (View Router display)	3-34	Preside MDM	2-6
launching		terminal server.	4-8
Preside MDM, client workstation	2-6	logging out	
WEBLink	3-55	terminal server.	4-18

M

maintenance access	4-16	software installation	5-3
Managed object (Session/Full Log column) . . .	3-19	minimum reboot time.	3-31
managing configuration data	5-1	modem	
managing security access in CiscoWorks2000 . .	1-2	backup	5-40
MDMWeb		restore.	5-40
accessing	2-49	viewing the configuration.	5-38
command line to WAN switch	2-53	monitoring	
displaying alarms	2-55	Ethernet port performance	1-19
navigating main window	2-52	LAN switch performance.	1-27
overview	2-47	MSFC routers	1-31
Microsoft HyperTerminal		system logs	1-26
channel bank backup and restore	5-26	MSFC routers, monitoring	1-31
Ethernet switch backup and restore	5-35		

N

navigating		new images, adding to library	1-52
MDMWeb main window	2-52	No radio button (Perform Checksum display). . .	3-39
terminal server menus	4-5	Now+ radio button (Reboot display)	3-29
Network Viewer	2-38		

O

Object Model (View Router display).	3-34	opening terminal server sessions, multiple	
obtaining the WAN switch name.	2-8	devices	4-12
		overview	

MDMWeb features. 2-47

Router Manager UI features. 3-1

P

password file

- capturing from routers 3-17
- checksumming. 3-39
- downloading to routers 3-14

Password file check box (Capture display) 3-18

Password File check box (Download display). . . 3-16

Password File check box (Perform Checksum display) 3-39

Perform Checksum display 3-38

performance information

- collecting 2-34
- displaying 2-34

performance monitoring

- Ethernet ports 1-19
- LAN switch 1-27
- MSFC routers 1-31
- real-time 2-34
- real-time statistics for LAN switch 1-10
- viewing router reports 3-58
- WAN switch and CPU memory utilization . . . 2-34

Performance Viewer

- collecting statistics on the WAN switch 2-34
- useful commands for 2-37

performing inventory on WAN switch 2-9

portal, firmware/software

- overview 3-45
- portal software overview 3-48
- upgrade procedure for EOS router firmware . . 3-46
- using to upgrade EOS firmware 3-49

prerequisites for router management 3-9

Preside MDM

- accessing 2-4
- displaying alarms 2-42
- fault management 2-44
- launching from client workstation 2-6
- managing security access 2-2
- menu options 2-6
- relaunching from client workstation 2-8
- security access, managing 2-2
- system diagram 2-4

Primary radio button (Capture display)

- capturing (uploading) files procedure 3-17

Primary radio button (Download display)

- downloading boot image, primary boot directory 3-52
- downloading files from the server 3-16
- downloading new EOS software, primary directory 3-42

Primary radio button (Perform Checksum display) 3-38

Primary radio button (Reboot display)

- after a specified interval 3-28
- at specified time 3-30
- immediate reboot 3-26

Primary radio button (Set Boot Block display) . . 3-33

Primary w/Test radio button

- immediate reboot 3-26

Primary w/Test Reboot radio button (Reboot display)

- verifying the software upgrade 3-43

provisioning mode 2-13

pseudo groups

- adding a router. 3-10

R

reboot directory

- setting. 3-32

Reboot display

- after a specified interval 3-29
- canceling a scheduled reboot 3-32
- immediate reboot procedure 3-25
- rebooting routers to update portal 3-53
- software upgrade procedure. 3-43

Reboot Now+ pull-down menu 3-29

reboot time

- minimum 3-31

- specifying 3-31
- specifying to occur after a specified interval . . 3-29

Reboot Time (Reboot display)

- after a specified interval 3-29
- immediate reboot 3-26
- verifying the software upgrade 3-43

rebooting routers 3-25

- after a scheduled interval 3-28
- at a scheduled time. 3-29
- immediately 3-25
- with test reboot option 3-26

- relaunching Preside MDM
 - client workstation 2-8
- reports
 - inventory on the WAN switch 2-9
 - viewing performance reports on routers 3-58
- resetting
 - card on WAN switch 2-45
 - Ethernet module 1-33
- Resource Manager Essentials
 - accessing 1-36
 - adding new images to library 1-52
 - applications 1-37
 - backing up configuration 1-42
 - backing up LAN switch software 1-42
 - Catalyst image files, copying to server 1-50
 - Catalyst image files, copying to TNM client 1-50
 - checking device configuration changes
 - Startup vs. Running example 1-63
 - two versions of same device example 1-59
 - copying Catalyst image files to server 1-50
 - copying Catalyst image files to TNM client 1-50
 - device configuration changes
 - verifying who made 1-65
 - device configuration changes, checking
 - Startup vs. Running example 1-63
 - two versions of same device example 1-59
 - distributing software images to LAN switch or MSFC router 1-54
 - LAN switch configuration restore 1-42
 - library, adding new images to 1-52
 - new software transfer to switch 1-49
 - procedures overview 1-35
 - restoring LAN switch configuration 1-42
 - software images, distributing to LAN switch or MSFC routers 1-54
 - transferring new software to switch 1-49
 - verifying who made changes 1-65
 - viewing LAN switch configuration 1-39
- Restore display 3-24
- Restore this Backup field (Restore display) 3-24
- restoring
 - ARCA-DACS 5-19
 - channel bank 5-30
 - DSU/CSU 5-33
 - Ethernet switch 5-37
 - files to the FullVision INM server 3-24 to 3-25
 - files to the FullVision server 3-23
 - LAN switch configuration 1-42
 - modem 5-40
 - terminal server 4-24
 - TRAK 9100 5-42
 - WAN switch 2-16
- resuming a terminal server session 4-14
- Router Cmd Log check box (Perform Checksum display) 3-39
- router command log
 - capturing from routers 3-17
 - checksumming 3-39
 - viewing 3-37
- Router Command Log check box (Capture display) 3-18
- router configuration
 - sample 3-10
 - viewing 3-59
- Router Configuration file filed (Add Router display) 3-11
- Router Directory (Perform Checksum display) 3-38
- router files, viewing 3-37
- Router Manager Reboot At option 3-30
- Router Manager UI
 - differences from WEBLink 3-55
 - overview 3-1
- Router Source Directory (Capture display) 3-17
- Router SysName field (Add Router display) 3-11
- routers
 - adding 3-10
 - boot blocks, configuring 3-10
 - Capture function defined 3-16
 - capturing (uploading) files procedure 3-17
 - command log capture from 3-17
 - Delete Router option 3-36
 - deleting 3-12
 - downloading files 3-15
 - overview of downloading files 3-14
 - preparing for management 3-9
 - preparing to add 3-9
 - preparing to delete 3-9
 - rebooting 3-25
 - rebooting after a scheduled interval 3-28
 - rebooting at a scheduled time 3-29
 - rebooting immediately 3-25
 - rebooting with test reboot option 3-26
 - View Router display 3-34
 - viewing configuration 3-59
 - viewing files for 3-37
 - viewing information about 3-33
- runtime logs 3-18
- resizing 3-19
- sorting 3-19
- viewing 3-18

S

S Series S4000 Hardware User Guide	3-2	CMT	5-14
scheduled reboots		HyperTerminal.	5-3
canceling	3-32	TFTP	5-7
two ways	3-27	software upgrades for routers in the field	3-40
Secondary radio button (Capture display)	3-17	software, transferring to switch	1-49
Secondary radio button (Download display)		Source Directory (Set Boot Block display)	3-33
downloading boot image to secondary boot		ST5000 Series Hardware User Guide	3-2
directory	3-51	SW Package Pri (View Router display).	3-34
downloading EOS software to secondary		SW Package Sec (View Router display)	3-34
directory	3-45	SW Version Pri (View Router display)	3-34
downloading files from the server	3-16	SW Version Sec (View Router display).	3-34
Secondary radio button (Perform Checksum		switch	
display)	3-38	backing up and restoring the WAN switch	2-11
Secondary radio button (Reboot display)		backing up ARCA-DACS	5-14
after a specified interval	3-28	backing up Ethernet switch	5-35
at scheduled time.	3-30	backing up LAN switch software	1-42
immediate reboot	3-26	downloading software to the WAN switch	2-18
Secondary radio button (Set Boot Block		restoring Ethernet switch	5-37
display)	3-33	transferring new software to LAN switch	1-49
security access in CiscoWorks2000	1-2	upgrading LAN switch software.	1-49
server logs	3-19	SysconF command	
Session (Session/Full Log column)	3-19	verifying router boot source settings	3-47
Session Log display	3-18	verifying the router boot source	3-50
viewing	3-19	SysIP Address (View Router display)	3-34
session, disconnecting a device session.	4-17	SysName/MO (View Router display)	3-34
Set Boot Block display	3-33	system diagram	
Severity (Session/Full Log column)	3-19	Preside MDM	2-4
SNMP community strings		Router Manager	3-3
assigning to router	3-10	system information, viewing for LAN switch.	1-14
software		system logs	
distributing images to LAN switch or MSFC		creating	1-23
router	1-54	monitoring.	1-26
downloading to WAN switch	2-18	system name, assigning to router	3-9
verifying LAN switch image distribution	1-58	system performance, impacts	1-1
software installation		system time, viewing	1-15

T

Target Directory (Download display)	3-45	launching from the View Router display	3-34
downloading boot image to primary		starting a Telnet session	3-36
directory	3-52	Telnet session to host	4-13
downloading EOS software to primary boot		Telnet, using with terminal server	4-7
directory	3-42	terminal server	
downloading files from the server to the		accessing	4-8
routers	3-16	accessing the maintenance environment	4-16
Telnet button (View Router display)		accessing through Telnet	4-7
starting a Telnet session	3-36	backing up.	4-20
Telnet session for a router		command keys.	4-5

dialing in	4-7	restoring factory defaults	4-24
disconnecting a session	4-17	resuming an open session	4-14
displaying users	4-15	viewing the configuration	4-19
logging out	4-18	test reboot option	3-26
main menu	4-10	TFTP, setup	5-3
opening a Telnet session with a host	4-13	three-copy backup rule	5-2
opening multiple sessions	4-12	TRAK 9100	
process	4-4	backing up and restoring	5-42
reasons for using	4-3	viewing the configuration	5-41
restoring	4-24	transferring new software to LAN switch	1-49

U

upgrading EOS software		procedure	3-17
portal overview	3-45	user file	
procedure with portal	3-46	capturing from routers	3-17
recommended procedure for field upgrade	3-40	checksumming	3-39
uploading files from routers		downloading to routers	3-14
Capture function	3-16		

V

verifying		channel bank configuration	5-26
installation of software images	1-58	CiscoWorks2000 account permissions	1-3
WAN switch addition	2-28	Ethernet switch configuration	5-34
who made device configuration changes	1-65	LAN switch configuration	1-39
View File button (View Router display)	3-37	modem configuration	5-38
View Router display		performance reports on routers	3-58
deleting a router	3-12	router configuration	3-59
launching WEBLink	3-55	status of WAN switch components	2-38
verifying the boot source of the router	3-50	system information	1-14
viewing router information and launching		system time	1-15
configuration applications	3-35	terminal server configuration	4-19
View Server Log submenu	3-20	TRAK 9100 configuration	5-41
viewing		VLAN members, displaying	1-17

W

WAN switch		obtaining the name	2-8
adding	2-23	obtaining the provisioning mode	2-13
backing up data	2-14	performing inventory on	2-9
connecting by command line	2-29	resetting card on	2-45
connecting by command line from client		restoring data	2-16
workstation	2-30	verifying the switch was added correctly	2-28
connecting by command line using		viewing status of	2-38
MDMWeb	2-53	WEBLink	
downloading software to	2-18	differences from Router Manager UI	3-55

launching	3-55	links	3-57
launching against a router.	3-36	using button in View Router display	3-56
launching from Router Manager.	3-34	WEBLink button (View Router display)	3-36
launching main window	3-56		

Y

Yes radio button (Perform Checksum display) . .	3-39
Yes, Verbose radio button (Perform Checksum display)	3-39

Z

zAllRouters group		Zhone CMT	
adding routers	3-10	software installation	5-14



MOTOROLA and the Stylized M Logo are registered in the U.S. Patent and Trademark Office. All other product or service names are the property of their respective owners.
© Motorola, Inc. 2002